KASPERSKY LAB

Kaspersky Anti-Virus 7.0

BENUTZERHANDBUCH

KASPERSKY ANTI-VIRUS 7.0

Benutzerhandbuch

© Kaspersky Lab
http://www.kaspersky.com/de

Erscheinungsdatum: December 2007

Inhalt

KAPITEL 1. BEDROHUNGEN FÜR DIE COMPUTERSICHERHEIT 9
1.1. Bedrohungsquellen 9
1.2. Ausbreitung der Bedrohungen 10
1.3. Arten von Bedrohungen 12
1.4. Kennzeichen einer Infektion 15
1.5. Was tun, wenn Kennzeichen einer Infektion auftreten? 16
1.6. Sicherheitsregeln 17

KAPITEL 2. KASPERSKY ANTI-VIRUS 7.0 20
2.1. Was ist neu bei Kaspersky Anti-Virus 7.0 20
2.2. Die Schutzprinzipien von Kaspersky Anti-Virus 23
2.2.1. Echtzeitschutz-Komponenten 23
2.2.2. Aufgaben zur Virensuche 25
2.2.3. Update 25
2.2.4. Servicefunktionen des Programms 26
2.3. Hardware- und Softwarevoraussetzungen 27
2.4. Lieferumfang 28
2.5. Service für registrierte Benutzer 29

KAPITEL 3. INSTALLATION VON KASPERSKY ANTI-VIRUS 7.0 30
3.1. Installation mit Hilfe des Assistenten 30
3.2. Konfigurationsassistent 35
3.2.1. Verwendung von Objekten, die in Version 5.0 gespeichert wurden 36
3.2.2. Aktivierung des Programms 36
3.2.2.1. Auswahl der Aktivierungsmethode 37
3.2.2.2. Eingabe des Aktivierungscodes 37
3.2.2.3. Registrierung des Benutzers 38
3.2.2.4. Download der Schlüsseldatei 38
3.2.2.5. Auswahl einer Schlüsseldatei 39
3.2.2.6. Abschluss der Programmaktivierung 39
3.2.3. Auswahl des Schutzmodus 39
3.2.4. Konfiguration der Update-Einstellungen 40

3.2.5. Konfiguration des Zeitplans für die Virenuntersuchung 41
3.2.6. Zugriffsbegrenzung für die Anwendung 42
3.2.7. Integritätskontrolle für Anwendungen 43
3.2.8. Abschluss des Konfigurationsassistenten 43
3.3. Installation der Anwendung aus der Befehlszeile 43

KAPITEL 4. PROGRAMMOBERFLÄCHE 45
4.1. Symbol im Infobereich der Taskleiste von Microsoft Windows 45
4.2. Kontextmenü 46
4.3. Programmhauptfenster 48
4.4. Konfigurationsfenster des Programms 53

KAPITEL 5. ERSTE SCHRITTE 55
5.1. Welchen Schutzstatus hat der Computer? 55
5.2. Status einer bestimmten Schutzkomponente 58
5.3. Wie der Computer auf Viren untersucht wird 59
5.4. Wie kritische Computerbereiche untersucht werden 59
5.5. Wie eine Datei, ein Ordner oder ein Laufwerk auf Viren untersucht werden 60
5.6. Wie das Programm aktualisiert wird 61
5.7. Was tun, wenn der Schutz nicht funktioniert? 62

KAPITEL 6. KOMPLEXE STEUERUNG DES SCHUTZES 63
6.1. Echtzeitschutz des Computers deaktivieren/aktivieren 63
6.1.1. Schutz anhalten 64
6.1.2. Computerschutz vollständig deaktivieren 65
6.1.3. Einzelne Schutzkomponenten anhalten/beenden 66
6.1.4. Computerschutz wiederherstellen 67
6.2. Technologie zur Desinfektion einer aktiven Infektion 67
6.3. Arbeit der Anwendung auf einem Laptop 68
6.4. Leistung des Computers beim Ausführen von Aufgaben 68
6.5. Lösen von Kompatibilitätsproblemen von Kaspersky Anti-Virus mit anderen Anwendungen 69
6.6. Start von Untersuchungs- und Update-Aufgaben mit Rechten eines anderen Benutzers 70
6.7. Konfiguration des Zeitplans für Aufgabenstart und Senden von Benachrichtigungen 71
6.8. Typen der zu kontrollierenden schädlichen Programme 73
6.9. Aufbau einer vertrauenswürdigen Zone 75

6.9.1. Ausnahmeregeln 76
6.9.2. Vertrauenswürdige Anwendungen 81

KAPITEL 7. VIRENSCHUTZ FÜR DAS DATEISYSTEM DES COMPUTERS 86
7.1. Auswahl der Sicherheitsstufe für den Dateischutz 87
7.2. Konfiguration des Dateischutzes 89
7.2.1. Festlegen der Typen von zu untersuchenden Dateien 89
7.2.2. Festlegen des Schutzbereichs 92
7.2.3. Anpassen zusätzlicher Parameter 95
7.2.4. Verwendung von heuristischen Analysemethoden 98
7.2.5. Wiederherstellen der Standardparameter für den Dateischutz 100
7.2.6. Auswahl der Aktion für Objekte 101
7.3. Aufgeschobene Desinfektion von Objekten 103

KAPITEL 8. E-MAIL-VIRENSCHUTZ 104
8.1. Auswahl der E-Mail-Sicherheitsstufe 105
8.2. Konfiguration des E-Mail-Schutzes 107
8.2.1. Auswahl der zu schützenden Richtung der Nachrichten 108
8.2.2. Anpassen der E-Mail-Untersuchung in Microsoft Office Outlook 110
8.2.3. Anpassen der E-Mail-Untersuchung in The Bat! 112
8.2.4. Verwendung von heuristischen Analysemethoden 114
8.2.5. Wiederherstellen der Standardparameter für den Mail-Schutz 115
8.2.6. Auswahl der Aktion für ein gefährliches E-Mail-Objekt 116

KAPITEL 9. WEB-SCHUTZ 119
9.1. Auswahl der Web-Sicherheitsstufe 121
9.2. Konfiguration des Web-Schutzes 123
9.2.1. Allgemeine Untersuchungsparameter 123
9.2.2. Erstellen einer Liste der vertrauenswürdigen Adressen 125
9.2.3. Verwendung von heuristischen Analysemethoden 126
9.2.4. Wiederherstellen der Standardparameter für den Web-Schutz 127
9.2.5. Auswahl der Aktion für ein gefährliches Objekt 128

KAPITEL 10. PROAKTIVER SCHUTZ FÜR IHREN COMPUTER 130
10.1. Regeln für die Aktivitätskontrolle 135
10.2. Integritätskontrolle für Anwendungen 139
10.2.1. Konfiguration von Kontrollregeln für kritische Anwendungen 140
10.2.2. Erstellen einer Liste der gemeinsamen Komponenten 143

10.3. Kontrolle über Veränderungen der Systemregistrierung 144
10.3.1. Auswahl von Registrierungsobjekten zum Erstellen einer Regel 146
10.3.2. Erstellen einer Regel zur Kontrolle von Registrierungsobjekten..... 147

KAPITEL 11. VIRENSUCHE AUF DEM COMPUTER 150
11.1. Steuerung von Aufgaben zur Virensuche 151
11.2. Erstellen einer Liste der Untersuchungsobjekte..... 152
11.3. Erstellen von Aufgaben zur Virensuche 153
11.4. Konfiguration von Aufgaben zur Virensuche..... 155
11.4.1. Auswahl der Sicherheitsstufe..... 156
11.4.2. Festlegen der zu untersuchenden Objekttypen 157
11.4.3. Zusätzliche Optionen für die Virensuche..... 160
11.4.4. Suche nach Rootkits 162
11.4.5. Verwendung heuristischer Analysemethoden..... 164
11.4.6. Wiederherstellen der standardmäßigen Untersuchungseinstellungen .. 164
11.4.7. Auswahl der Aktion für Objekte..... 165
11.4.8. Festlegen einheitlicher Untersuchungsparameter für alle Aufgaben..... 167

KAPITEL 12. TESTEN DER ARBEIT VON KASPERSKY ANTI-VIRUS..... 169
12.1. EICAR-"Testvirus" und seine Modifikationen 169
12.2. Testen des Datei-Anti-Virus 171
12.3. Testen einer Aufgabe zur Virensuche 172

KAPITEL 13. UPDATE DES PROGRAMMS 174
13.1. Starten des Updates..... 176
13.2. Rollback zum vorherigen Update 176
13.3. Update-Einstellungen..... 177
13.3.1. Auswahl der Updatequelle 177
13.3.2. Auswahl von Updatemodus und Update-Objekt..... 180
13.3.3. Update-Verteilung..... 182
13.3.4. Aktionen nach dem Programm-Update..... 184

KAPITEL 14. SCHLÜSSELVERWALTUNG..... 185

KAPITEL 15. ZUSÄTZLICHE OPTIONEN 187
15.1. Quarantäne für möglicherweise infizierte Objekte 188
15.1.1. Aktionen mit Objekten in der Quarantäne 189
15.1.2. Konfiguration der Quarantäne-Einstellungen 192

15.2. Sicherungskopien gefährlicher Objekte ... 193
15.2.1. Aktionen mit Sicherungskopien ... 193
15.2.2. Konfiguration der Backup-Einstellungen ... 195
15.3. Berichte ... 195
15.3.1. Konfiguration der Berichtsparameter ... 198
15.3.2. Registerkarte *Gefunden* ... 199
15.3.3. Registerkarte *Ereignisse* ... 200
15.3.4. Registerkarte *Statistik* ... 202
15.3.5. Registerkarte *Einstellungen* ... 202
15.3.6. Registerkarte *Registrierung* ... 204
15.4. Notfall-CD zur Systemwiederherstellung ... 204
15.4.1. Erstellen einer Notfall-CD ... 205
15.4.2. Verwendung der Notfall-CD ... 207
15.5. Erstellen einer Liste der zu kontrollierenden Ports ... 209
15.6. Untersuchung geschützter Verbindungen ... 211
15.7. Konfiguration der Proxyserver-Parameter ... 213
15.8. Konfiguration der Oberfläche von Kaspersky Anti-Virus ... 215
15.9. Verwendung zusätzlicher Dienste ... 218
15.9.1. Benachrichtigungen über die Ereignisse von Kaspersky Anti-Virus ... 219
15.9.1.1. Ereignistypen und Methoden zum Senden von Benachrichtigungen ... 220
15.9.1.2. Konfiguration des Sendens von Benachrichtigungen per E-Mail ... 222
15.9.1.3. Parameter des Ereignisberichts ... 224
15.9.2. Selbstschutz und Zugriffsbeschränkung für das Programm ... 225
15.9.3. Export/Import der Einstellungen von Kaspersky Anti-Virus ... 227
15.9.4. Wiederherstellen der Standardeinstellungen ... 227
15.10. Technischer Support für Benutzer ... 228
15.11. Arbeit mit der Anwendung beenden ... 231

KAPITEL 16. ARBEIT MIT DEM PROGRAMM AUS DER BEFEHLSZEILE ... 233
16.1. Aktivierung der Anwendung ... 235
16.2. Steuerung von Anwendungskomponenten und Aufgaben ... 236
16.3. Virenuntersuchung von Objekten ... 239
16.4. Programm-Update ... 244
16.5. Rollback des letzten Updates der Anwendung ... 245
16.6. Export von Schutzparametern ... 246
16.7. Import von Schutzparametern ... 246

16.8. Anwendung starten 247
16.9. Anwendung beenden 247
16.10. Anlegen einer Tracing-Datei 247
16.11. Anzeige der Hilfe 248
16.12. Rückgabecodes der Befehlszeile 249

KAPITEL 17. PROGRAMM ÄNDERN, REPARIEREN ODER LÖSCHEN 250
17.1. Ändern, Reparieren oder Löschen des Programms mit Hilfe des Installationsassistenten 250
17.2. Deinstallation des Programms aus der Befehlszeile 252

KAPITEL 18. HÄUFIGE FRAGEN 254

ANHANG A. ZUSÄTZLICHE INFORMATIONEN 256
A.1. Liste der Objekte, die nach Erweiterung untersucht werden 256
A.2. Zulässige Ausschlussmasken für Dateien 259
A.3. Zulässige Ausschlussmasken nach der Klassifikation der Viren-Enzyklopädie 260

ANHANG B. KASPERSKY LAB 261
B.1. Weitere Produkte und Services von Kaspersky Lab 262
B.2. Kontaktinformationen 272

ANHANG C. ENDBENUTZER-LIZENZVERTRAG FÜR DIE ERWORBENE KASPERSKY LAB SOFTWARE 274

KAPITEL 1. BEDROHUNGEN FÜR DIE COMPUTERSICHERHEIT

Aufgrund der rasanten Entwicklung der Informationstechnologien und ihrer Präsenz in allen Lebensbereichen ist die Zahl der Cyber-Verbrechen stark gestiegen.

Auf besonderes Interesse von Cyber-Verbrechern stößt die Tätigkeit staatlicher Einrichtungen und kommerzieller Unternehmen. Ziele sind der Diebstahl, und der Verkauf vertraulicher Informationen, Rufschädigung, Schädigung der Netzwerke und Zugang zu Informationsressourcen einer Organisation. Solche Aktionen verursachen enormen materiellen Schaden und Imageverlust.

Diesem Risiko unterliegen nicht nur Großunternehmen, sondern auch private Nutzer. Mit Hilfe unterschiedlicher Mittel verschaffen sich Verbrecher Zugriff auf persönliche Daten wie Kontonummern, Kreditkartennummern und Kennwörter, machen das System funktionsunfähig oder erhalten vollständigen Zugang auf den Computer. Ein infizierter Computer kann als Teil eines so genannten Zombie-Netzes benutzt werden, eines Netzwerks von infizierten Computern, das dazu dient, Angriffe auf Server auszuüben, Spam zu versenden, vertrauliche Informationen zu sammeln sowie neue Viren und Trojaner zu verbreiten.

Es ist heute allgemein anerkannt, dass Informationen ein wertvolles Gut sind und geschützt werden müssen. Gleichzeitig sollen Informationen aber für einen bestimmten Kreis von Benutzern zugänglich sein (beispielsweise für Mitarbeiter, Kunden und Geschäftspartner). Deshalb ist ein komplexes System zur für die Informationssicherheit nötig. Dieses System muss alle bestehenden Bedrohungsquellen berücksichtigen (menschliche, technische und unvorhersehbare Faktoren) und das gesamte Spektrum von Schutzmaßnahmen verwenden, wozu physikalische, administrative und mit Software und Technik verbundene Schutzwerkzeuge zählen.

1.1. Bedrohungsquellen

Als Quellen für die Bedrohung der Informationssicherheit können eine Einzelperson oder eine Personengruppe, sowie Phänomene, die von menschlicher Tätigkeit unabhängig sind, auftreten. Dadurch lassen sich drei Gruppen von Bedrohungsquellen unterscheiden:

- **Menschlicher Faktor**. Diese Gruppe von Bedrohungen steht mit den Aktionen eines Menschen in Verbindung, der rechtmäßigen oder uner-

laubten Zugriff auf Informationen besitzt. Die Bedrohungen dieser Gruppe können unterteilt werden in:

- *externe*: Dazu zählen Aktionen von Cyber-Verbrechern, Hackern, Internetbetrügern und böswilligen Partnern.
- *interne*: Hierzu gehören die Aktionen von Firmenmitarbeitern und PC-Benutzern. Die Handlungen dieser Personen können vorsätzlich oder zufällig sein.

- **Technischer Faktor**. Diese Gruppe von Bedrohungen ist mit technischen Problemen verbunden. Dazu zählen veraltete Geräte sowie mindere Qualität der benutzten Software und Hardware. Diese Faktoren können zur Fehlfunktion von Geräten und zum teilweisen Verlust von Informationen führen.
- **Unvorhersehbarer Faktor**. Diese Gruppe der Bedrohungen umfasst Naturkatastrophen und sonstige Umstände höherer Gewalt, die nicht von menschlicher Tätigkeit abhängig sind.

Alle drei Bedrohungsquellen sollten bei der Organisation eines Schutzsystems berücksichtigt werden. In diesem Handbuch beschreiben wir allerdings nur eine Quelle, die direkt mit der Tätigkeit der Firma Kaspersky Lab verbunden ist: die externen Bedrohungen, die mit menschlicher Tätigkeit in Verbindung stehen.

1.2. Ausbreitung der Bedrohungen

Die Entwicklung der modernen Computertechnologien und Kommunikationsmittel verleiht Angreifern die Möglichkeit, unterschiedliche Verbreitungsquellen für Bedrohungen zu benutzen, die im Folgenden genauer beschrieben werden:

Internet

Das Internet zeichnet sich dadurch aus, dass es niemandem gehört und keine territorialen Grenzen besitzt. Das ermöglicht die Entwicklung zahlreicher Web-Ressourcen und den Austausch von Informationen. Jeder Mensch kann Zugriff auf die im Internet gespeicherten Daten erhalten oder seinen eigenen Online-Service anbieten.

Allerdings wird Angreifern eben durch diese Besonderheiten ermöglicht, im Internet Verbrechen zu verüben, die nur schwer erkannt und verfolgt werden können.

Böswillige Personen platzieren Viren und andere Schadprogramme auf Webseiten und tarnen diese als nützliche und kostenlose Software. Außerdem können Skripts, die beim Öffnen bestimmter Webseiten automatisch gestartet werden, schädliche Aktionen auf dem Computer ausführen, wozu

Modifikation der Systemregistrierung, Diebstahl persönlicher Daten und Installation schädlicher Programme gehören.

Mit Netzwerktechnologien verwirklichen lassen sich Angriffe auf entfernte PCs und Unternehmensserver verwirklichen. Das Ergebnis solcher Angriffe kann die Funktionsuntüchtigkeit der Ressource, der vollständige Zugriff auf die darauf gespeicherten Informationen sowie der Missbrauch des Rechners als Teil eines Zombie-Netzes sein.

Im Bereich Kreditkartenzahlung, E-Money und Online-Banking (Internet-Shops, -Auktionen, Websites von Banken usw.) hat sich der Internetbetrug zu einem weit verbreiteten Verbrechen entwickelt.

Intranet

Das Intranet ist ein lokales Netzwerk, das den speziellen Erfordernissen der Informationsverwaltung in einem Unternehmen oder in einem privaten Netzwerk entspricht. Ein Intranet stellt einen einheitlichen Raum zum Speichern, Austausch und Zugriff auf Informationen für alle Computer eines Netzwerks dar. Ist ein Computer des Netzwerks infiziert, dann unterliegen die übrigen Computer einem ernsten Infektionsrisiko. Um das zu verhindern, müssen nicht nur die Grenzen des Netzwerks geschützt werden, sondern auch jeder einzelne Computer.

E-Mail

Da praktisch auf jedem Computer ein Mailprogramm installiert ist und schädliche Programme auf der Suche nach neuen Opfern den Inhalt elektronischer Adressbücher verwenden, entstehen günstige Bedingungen für die Ausbreitung von Schadprogrammen. Der Benutzer eines infizierten Computers verschickt - ohne selbst Verdacht zu schöpfen - infizierte E-Mails an Adressaten, die ihrerseits neue infizierte Mails weiterschicken usw. Häufig gelangt ein infiziertes Dokument oder eine Datei durch Unachtsamkeit in eine Verteilerliste für kommerzielle Informationen eines Großunternehmens. In diesem Fall sind nicht nur fünf, sondern hunderte oder tausende von Abonnenten solcher Verteiler betroffen, welche die infizierten Dateien wiederum an zehntausende ihrer Abonnenten weiterreichen.

Neben der Gefahr des Eindringens von Schadprogrammen besteht das Problem unerwünschter E-Mails, die Werbung enthalten (Spam). Zwar stellen unerwünschte E-Mails keine direkte Bedrohungsquelle dar, doch erhöhen sie die Belastung von Mailservern, ergeben zusätzlichen Datenverkehr, verstopfen das Benutzerpostfach, führen zu Zeitverlust und verursachen dadurch erhebliche finanzielle Schäden.

Erwähnenswert ist auch, dass Angreifer so genannte Spam-Technologien mit Massencharakter und Methoden des Social Engineering verwenden, um einen Benutzer dazu zu veranlassen, eine E-Mail zu öffnen, über einen Link aus der E-Mail zu einer bestimmten Internetressource zu gehen usw. Des-

halb ist die Möglichkeit zur Spam-Filterung auch zum Kampf gegen neue Arten des Internetbetrugs (wie beispielsweise Phishing) sowie gegen die Verbreitung von Schadprogrammen notwendig.

Wechseldatenträger

Zum Speichern und zur Weitergabe von Informationen sind CDs/DVDs, Disketten und Speichererweiterungskarten (Flash-Card) weit verbreitet.

Wenn Sie eine Datei, die schädlichen Code enthält, von einem Wechseldatenträger starten, können die auf Ihrem Computer gespeicherten Daten beschädigt werden und ein Virus kann sich auf andere Computerlaufwerke oder Netzwerkcomputer ausbreiten.

1.3. Arten von Bedrohungen

Heutzutage existiert eine große Menge von Bedrohungen, denen Ihr Computer ausgesetzt ist. Dieser Abschnitt bietet eine ausführliche Beschreibung der Bedrohungen, die von Kaspersky Anti-Virus blockiert werden:

Würmer

Diese Kategorie der schädlichen Programme benutzt in erster Linie die Schwachstellen von Betriebssystemen, um sich auszubreiten. Die Klasse erhielt ihren Namen aufgrund ihrer wurmähnlichen Fähigkeit, von Computer zu Computer "weiter zu kriechen", wobei Netzwerke und E-Mails benutzt werden. Deshalb besitzen Würmer eine relativ hohe Ausbreitungsgeschwindigkeit.

Würmer dringen in einen Computer ein, suchen nach Netzwerkadressen anderer Computer und versenden ihre Kopien an diese Adressen. Neben Netzwerkadressen verwenden Würmer häufig auch Daten aus dem Adressbuch von Mailprogrammen. Vertreter dieser Klasse der schädlichen Programme erstellen teilweise Arbeitsdateien auf Systemlaufwerken, können aber auch ohne jeden Zugriff auf Computerressourcen (mit Ausnahme des Arbeitsspeichers) funktionieren.

Viren

Viren sind Programme, die andere Programme infizieren, indem sie ihnen den eigenen Code hinzufügen, um beim Start infizierter Dateien die Kontrolle zu übernehmen. Diese einfache Definition nennt die *Infektion* als von einem Virus ausgeführte Basisaktion.

Trojaner

Trojaner sind Programme, die auf infizierten Computern unerlaubte Aktionen ausführen, d.h. abhängig von bestimmten Bedingungen die Informationen auf Laufwerken vernichten, das System zum Absturz bringen, vertrauliche

Informationen stehlen usw. Diese Klasse der schädlichen Programme fällt nicht unter die traditionelle Definition eines Virus (d.h. andere Programme oder Daten werden nicht infiziert). Trojanische Programme können nicht selbständig in einen Computer eindringen. Sie werden getarnt als nützliche Software verbreitet. Dabei kann der verursachte Schaden den eines traditionellen Virusangriffs erheblich übersteigen.

In letzter Zeit haben sich Würmer zum häufigsten Typ der Schadprogramme entwickelt, danach folgen Viren und Trojaner. Einige schädliche Programme verbinden die Merkmale von zwei oder gar drei der oben genannten Klassen.

Adware

Adware sind Programme, die ohne Wissen des Benutzers in anderer Software enthalten sind und die Präsentation von Werbung zum Ziel haben. In der Regel ist Adware in Programme integriert, die kostenlos verbreitet werden. Die Werbung erscheint auf der Benutzeroberfläche. Häufig sammeln solche Programme persönliche Benutzerdaten und senden Sie an den Programmautor, ändern bestimmte Browser-Einstellungen (Start- und Such-Seiten, Sicherheitsstufe u.a.), und verursachen vom Benutzer unkontrollierten Datenverkehr. Dadurch kann die Sicherheitsrichtlinie verletzt werden und es können direkte finanzielle Verluste entstehen.

Spyware

Spyware sammelt heimlich Informationen über einen bestimmten Benutzer oder eine Organisation. Die Existenz von Spyware auf einem Computer kann völlig unbemerkt bleiben. In der Regel verfolgt Spyware folgende Ziele:

- Überwachen der Benutzeraktionen auf einem Computer
- Sammeln von Informationen über den Festplatteninhalt. In diesem Fall werden meistens bestimmte Ordner und die Systemregistrierung des Computers gescannt, um eine Liste der installierten Software zu erstellen.
- Sammeln von Informationen über Verbindungsqualität, Verbindungsmethode, Modemgeschwindigkeit usw.

Potentiell gefährliche Anwendungen (Riskware)

Als potentiell gefährlich gelten Anwendungen, die nicht über schädliche Funktionen verfügen, die aber Teil der Entwicklungsumgebung eines Schadprogramms sein können oder von Angreifern als Hilfskomponenten schädlicher Programme verwendet werden können. Zu dieser Kategorie zählen Programme, die Schwachstellen und Fehler enthalten, sowie Dienstprogramme zur Remote-Administration, Programme zum automatischen Umschalten der Tastaturbelegung, IRC-Clients, FTP-Server und alle Dienstprogramme zum Beenden von Prozessen oder zum Verstecken der Arbeit von Prozessen.

Ein weiterer Typ von Schadprogrammen, die solchen Programmen wie Adware, Spyware und Riskware nahe stehen, sind Programme die in den auf einem Computer installierten Browser integriert werden. Vielleicht sind Sie schon auf solche Programme gestoßen, wenn beim Aufruf einer Webseiten-Adresse eine ganz andere Seite geöffnet wurde.

Scherzprogramme (Jokes)

Jokes sind Software, die dem Computer keinen direkten Schaden zufügt, sondern Meldungen darüber anzeigen, dass Schaden verursacht wurde oder unter bestimmten Bedingungen verursacht wird. Solche Programme warnen den Benutzer häufig vor fiktiven Gefahren. So kann beispielsweise eine Meldung angezeigt werden, die über das Formatieren der Festplatte informiert (obwohl dies nicht der Wirklichkeit entspricht) oder einen Virusfund in Dateien meldet, die aber tatsächlich virenfrei sind.

Rootkits

Rootkits sind Dienstprogramme, die der Tarnung von Prozessen dienen. Sie maskieren auch schädliche Programme, um zu vermeiden, dass diese von Antiviren-Programmen gefunden werden. Rootkits sind außerdem fähig, das Betriebssystem des Computers zu modifizieren und dessen Grundfunktionen zu ersetzen, wodurch sie die eigene Existenz und Aktionen, die ein Angreifer auf dem infizierten Computer vornimmt, verbergen.

Andere gefährliche Programme

Dazu zählen Programme, die der Organisation von DoS-Angriffen auf entfernte Server, dem Eindringen in andere Computer und dem Erstellen schädlicher Software dienen. Zu diesen Programmen gehören Hackerdienstprogramme (Hack-Tools), Virenautoren, Schwachstellen-Scanner, Programme zum Kennwort-Diebstahl sowie sonstige Programme zum Einbruch in Netzwerkressourcen oder zum Eindringen in ein angegriffenes System.

Das Erkennen und Blockieren dieser Arten von Bedrohungen wird von Kaspersky Anti-Virus mit Hilfe von zwei Methoden ausgeführt:

- *reaktiv* – Diese Methode beruht auf der Suche von schädlichen Objekten mit Hilfe der regelmäßig aktualisierten Programm-Datenbanken. Zur Realisierung dieser Methode muss mindestens eine Infektion erfolgt sein, wonach den Datenbanken die entsprechende Bedrohungssignatur hinzugefügt und das Update der Datenbanken weitergegeben werden kann.
- *proaktiv* – Im Unterschied zum reaktiven Schutz basiert diese Methode nicht auf der Code-Analyse eines Objekts, sondern auf der Analyse seines Verhaltens im System. Diese Methode ermöglicht das Erkennen neuer Gefahren, über die noch keine Informationen in den Datenbanken vorhanden sind.

Die Verwendung beider Methoden in Kaspersky Anti-Virus gewährleistet den kompletten Schutz Ihres Computers vor bekannten und neuen Bedrohungen.

Achtung!

Ab hier wird in diesem Handbuch zur Bezeichnung von schädlichen und gefährlichen Programmen der Begriff "Virus" verwendet. Die konkrete Art eines Schadprogramms wird nur dann extra genannt, wenn es erforderlich ist.

1.4. Kennzeichen einer Infektion

Es existiert eine Reihe von Kennzeichen, die auf eine Computerinfektion hinweisen. Wenn Sie bemerken, dass sich der Computer beispielsweise auf folgende Weise "seltsam" verhält, dann ist er mit hoher Wahrscheinlichkeit von einem Virus infiziert:

- Es werden unvorhergesehene Meldungen oder Bilder auf dem Bildschirm angezeigt oder unvorhergesehene Audiosignale wiedergegeben.
- Die Schublade des CD/DVD-ROM-Laufwerks öffnet und schließt sich ohne erkennbaren Grund.
- Bestimmte Programme auf dem Computer werden willkürlich gestartet, ohne dass dies von Ihnen initiiert wurde.
- Auf dem Bildschirm werden Meldungen angezeigt, die sich auf den Versuch bestimmter Programme Ihres Computers beziehen, eine Verbindung mit dem Internet herzustellen, obwohl Sie dies nicht initiiert haben.

Außerdem gibt es einige charakteristische Merkmale für eine Virusinfektion durch E-Mails:

- Freunde oder Bekannte teilen Ihnen mit, dass sie Nachrichten von Ihnen erhalten haben, die Sie aber nicht abgeschickt haben.
- In Ihrer Mailbox befindet sich eine große Anzahl von Nachrichten ohne Antwortadresse und Betreff.

Es ist anzumerken, dass diese Merkmale nicht immer durch die Existenz von Viren hervorgerufen werden. Manchmal können sie auf andere Ursachen zurückgehen. So können beispielsweise infizierte Nachrichten zwar Ihre Adresse als Antwortadresse enthalten, aber trotzdem von einem anderen Computer aus abgeschickt worden sein.

Außerdem existieren indirekte Hinweise auf eine Infektion Ihres Computers:

- häufiges Abstürzen und Funktionsstörungen des Computers.

- verlangsamter Start von Programmen.
- das Laden des Betriebssystems ist nicht möglich.
- Verschwinden von Dateien und Ordnern oder Veränderungen ihres Inhalts.
- häufiger Zugriff auf die Festplatte (häufiges Blinken des Festplattenindikators am PC-Gehäuse).
- Der Webbrowser (z.B. Microsoft Internet Explorer) "bleibt hängen" oder verhält sich unerwartet (z.B. das Programmfenster lässt sich nicht schließen).

In 90 % der Fälle werden indirekte Symptome durch Hardware- oder Softwarestörungen verursacht. Trotz der geringen Wahrscheinlichkeit, dass solche Symptome auf eine Infektion zurückgehen, wird bei ihrem Auftreten empfohlen, den Computer vollständig zu untersuchen (s. 5.3 auf S. 59).

1.5. Was tun, wenn Kennzeichen einer Infektion auftreten?

Wenn Sie bemerken, dass sich Ihr Computer "verdächtig verhält",

1. Keine Panik! Diese goldene Regel kann Sie vor dem Verlust wichtiger Daten bewahren.
2. Trennen Sie den Computer vom Internet und vom lokalen Netzwerk, wenn er damit verbunden ist.
3. Wenn das Symptom darin besteht, dass der Systemstart von der Festplatte des Computers nicht möglich ist (der Computer gibt einen Fehler aus, wenn Sie ihn einschalten), versuchen Sie, das System im abgesicherten Modus oder von der Microsoft Windows-Rettungsdiskette zu starten, die Sie bei der Installation des Betriebssystems auf dem Computer erstellt haben.
4. Bevor Sie irgendwelche Aktionen ausführen, speichern Sie Ihre Daten auf einem externen Datenträger (Diskette, CD/DVD, Flash-Card usw.).
5. Installieren Sie Kaspersky Anti-Virus, falls er noch nicht installiert wurde.
6. Aktualisieren Sie die Programm-Datenbanken und die Programm-Module (s. 5.6 auf S. 61) des Programms. Verwenden Sie für den Download aus dem Internet möglichst nicht Ihren eigenen Computer, sondern einen virenfreien Computer (Computer eines Freundes, im Internet-Café, bei der Arbeit). Die Verwendung eines anderen Compu-

ters ist von Vorteil, da bei einer Internetverbindung des infizierten Computers die Möglichkeit besteht, dass der Virus wichtige Informationen an die Angreifer sendet oder sich an die Adressen Ihres Adressbuchs verschickt. Gerade deshalb sollte bei einem Infektionsverdacht die Verbindung mit dem Internet sofort getrennt werden.

7. Stellen Sie die von Kaspersky-Lab-Experten empfohlene Schutzstufe ein.
8. Starten Sie die vollständige Untersuchung des Computers (s. 5.3 auf S. 59).

1.6. Sicherheitsregeln

Selbst die zuverlässigsten und vernünftigsten Maßnahmen können keinen hundertprozentigen Schutz vor Computerviren und Trojanern bieten. Allerdings lässt sich das Risiko einer Virusinfektion und möglicher Verluste minimieren, indem Sie folgende Regeln beachten.

Eine der wichtigsten Methoden im Kampf gegen Viren ist, wie auch in der Medizin, die rechtzeitige *Prophylaxe*. Die Computerprophylaxe umfasst wenige Regeln, welche die Wahrscheinlichkeit einer Virusinfektion und des Datenverlusts erheblich verringern.

Im Folgenden finden Sie die wichtigsten Sicherheitsregeln die Ihnen helfen, das Risiko von Virenangriffen zu vermeiden.

Regel 1: *Schützen Sie Ihren Computer mit Hilfe eines Antiviren-Programms und einer Firewall*:

- Installieren Sie umgehend Kaspersky Anti-Virus.
- Aktualisieren Sie regelmäßig die Datenbanken, die zum Umfang des Programms gehören (s. 5.6 auf S. 61). Das Update kann beim Eintreten einer Virenepidemie mehrmals täglich vorgenommen werden. In solchen Fällen werden die Programm-Datenbanken auf den Kaspersky-Lab-Updateservern unverzüglich aktualisiert.
- Legen Sie die von den Kaspersky-Lab-Experten empfohlenen Einstellungen für den Schutz Ihres Computers fest. Der Echtzeitschutz wird sofort nach dem Hochfahren des Computers wirksam und erschwert Viren das Eindringen in den Computer.
- Legen Sie die von Kaspersky Lab empfohlenen Einstellungen für die vollständige Untersuchung des Computers fest und planen Sie deren Ausführung mindestens einmal pro Woche.

Regel 2: *Verhalten Sie sich beim Speichern neuer Daten auf dem Computer vorsichtig*:

- Untersuchen Sie alle Wechseldatenträger (s. 5.5 auf S. 60) (Disketten, CDs/DVDs-ROMs, Flash-Cards usw.) vor deren Verwendung auf das Vorhandensein von Viren.
- Gehen Sie vorsichtig mit E-Mail-Nachrichten um. Starten Sie nie Dateien, die Sie per E-Mail erhalten haben, wenn Sie nicht sicher sind, dass diese wirklich für Sie bestimmt sind, selbst wenn diese von einem Bekannten abgeschickt wurden.
- Gehen Sie vorsichtig mit allen Daten um, die Sie aus dem Internet empfangen haben. Wenn Ihnen von einer Webseite angeboten wird, ein neues Programm zu installieren, vergewissern Sie sich über das Vorhandensein eines Sicherheitszertifikats.
- Wenn Sie eine ausführbare Datei aus dem Internet oder über ein lokales Netzwerk herunterladen, dann untersuchen Sie diese unbedingt mit Kaspersky Anti-Virus.
- Verhalten Sie sich vorsichtig bei der Auswahl der von Ihnen besuchten Internetressourcen. Bestimmte Seiten sind von gefährlichen Skriptviren oder Internetwürmern infiziert.

Regel 3: *Verfolgen Sie aufmerksam die Informationen von Kaspersky Lab*.

In den meisten Fällen informiert Kaspersky Lab über den Ausbruch einer neuen Epidemie lange bevor diese ihren Höhepunkt erreicht. Die Wahrscheinlichkeit einer Infektion ist in diesem Fall noch gering und durch den Download der aktualisierten Programm-Datenbanken können Sie sich rechtzeitig vor einem neuen Virus schützen.

Regel 4: *Verhalten Sie sich misstrauisch gegenüber falschen Viruswarnungen, Scherzprogrammen und E-Mails, die vorgeben vor Infektionen zu warnen*.

Regel 5: *Verwenden Sie den Dienst Windows Update und installieren Sie regelmäßig die Updates für das Betriebssystem Microsoft Windows*

Regel 6: *Kaufen Sie Ihre Software nur bei offiziellen Händlern*.

Regel 7: *Beschränken Sie den Kreis der Leute, die zur Arbeit auf Ihrem Computer berechtigt sind*.

Regel 8: *Verringern Sie das Risiko unangenehmer Folgen einer möglichen Infektion*:

- Fertigen Sie rechtzeitig Sicherungskopien Ihrer Daten an. Wenn Sicherungskopien vorhanden sind, kann das System bei Datenverlust schnell wiederhergestellt werden. Distributions-CDs, Disketten, Flash-Cards und andere Datenträger mit Software und wertvollen Informationen sollten an einem sicheren Ort aufbewahrt werden.

- Erstellen Sie unbedingt eine Notfall-CD (s. 15.4 auf S. 204), von der Sie Ihren Computer bei Bedarf unter Verwendung eines "sauberen" Betriebssystems starten können.

Regel 9: *Überprüfen Sie regelmäßig die Liste der auf Ihrem Computer installierten Programme*. Dazu können Sie den Dienst **Programme ändern oder entfernen** in der **Systemsteuerung** verwenden oder den Inhalt des Ordners **Programme** und des Ordners Autostart prüfen. Dadurch können Sie Software finden, die ohne Ihr Wissen auf dem Computer installiert wurde, während Sie beispielsweise das Internet benutzt oder ein bestimmtes Programm installiert haben. Möglicherweise befinden sich potentiell gefährliche Programme darunter.

KAPITEL 2. KASPERSKY ANTI-VIRUS 7.0

Kaspersky Anti-Virus 7.0 ist die neue Generation des Informationsschutzes.

Der Hauptunterschied zwischen Kaspersky Anti-Virus 7.0 und anderen Produkten, einschließlich anderer Kaspersky-Lab-Produkte, besteht in der komplexen Methode zum Schutz der Daten auf dem Computer.

2.1. Was ist neu bei Kaspersky Anti-Virus 7.0

Kaspersky Anti-Virus 7.0 bietet eine prinzipiell neue Methode zum Datenschutz. Das wichtigste Merkmal des Programms besteht darin, dass verschiedene Funktionen in einer komplexen Lösung vereinigt und bedeutend optimiert wurden. Das Programm bietet nicht nur einen Virenschutz, sondern auch den Schutz vor unbekannten Bedrohungen.

Der komplexe Schutz wird auf allen Kanälen gewährleistet, auf denen Daten eingehen und übertragen werden. Die flexible Konfiguration aller Programmkomponenten erlaubt es, Kaspersky Anti-Virus genau an die Anforderungen eines konkreten Benutzers anzupassen. Außerdem können alle Schutzkomponenten unter einer Oberfläche konfiguriert werden.

Im Folgenden werden die neuen Optionen von Kaspersky Anti-Virus 7.0 ausführlich beschrieben.

Neuerungen im Schutz

- Kaspersky Anti-Virus schützt nicht nur vor bekannten schädlichen Programmen, sondern auch vor solchen, die noch unbekannt sind. Die Komponente Proaktiver Schutz (s. Kapitel 10 auf S. 130) stellt einen der wichtigsten Vorzüge des Programms dar. Ihre Arbeit beruht auf der Analyse des Verhaltens der auf Ihrem Computer installierten Anwendungen, der Kontrolle von Veränderungen in der Systemregistrierung und dem Kampf gegen versteckte Bedrohungen. Bei der Arbeit der Komponente wird eine heuristische Analyse verwendet, die es erlaubt, unterschiedliche Arten von Schadprogrammen zu erkennen. Hierbei wird ein Bericht geführt, auf dessen Basis Aktionen, die von Schadprogrammen ausgeführt wurden, rückgängig gemacht werden können und

der Systemszustand vor der schädlichen Veränderung wiederhergestellt werden kann.

- Die Technologie für den Schutz der Dateien auf dem Benutzercomputer wurde verbessert: Sie können nun die Belastung des Zentralprozessors und der Laufwerkssubsysteme senken und die Untersuchungsgeschwindigkeit erhöhen. Dies wird durch die Verwendung der Technologien iChecker™ und iSwift™ erreicht. Dieser Modus schließt die wiederholte Prüfung von Dateien aus.

- Der Prozess zur Virensuche wird nun Ihrer Arbeit auf dem Computer untergeordnet. Eine Untersuchung kann relativ viel Zeit und Systemressourcen beanspruchen, trotzdem kann der Benutzer gleichzeitig seine Arbeit ausführen. Wenn das Ausführen einer bestimmten Operation Systemressourcen erfordert, wird die Virensuche bis zum Abschluss dieser Operation angehalten. Danach wird die Untersuchung an der Stelle fortgesetzt, an dem sie angehalten wurde.

- Der Untersuchung von kritischen Computerbereichen und Autostart-Objekten, deren Infektion irreparable Folgen haben kann, sowie der Suche nach Rootkits, die Schadprogramme im System verstecken, sind separate Aufgaben zugeordnet. Sie können diese Aufgaben so konfigurieren, dass sie jedes Mal beim Hochfahren des Systems automatisch gestartet werden.

- Der Schutz von E-Mails vor schädlichen Programmen wurde wesentlich verbessert. Das Programm untersucht den E-Mailstrom folgender Protokolle auf Viren:

  - IMAP, SMTP, POP3, unabhängig vom verwendeten Mailprogramm.

  - NNTP unabhängig vom verwendeten Mailprogramm.

  - unabhängig vom Protokolltyp (einschließlich MAPI, HTTP) im Rahmen der Arbeit der in die Mailprogramme Microsoft Office Outlook und The Bat! integrierten Plug-ins.

- In bekannte Mailprogramme wie Microsoft Office Outlook, Microsoft Outlook Express (Windows Mail) und The Bat! wird ein spezielles Erweiterungsmodul (Plug-in) integriert, das die Konfiguration des E-Mail-Schutzes direkt im Mailprogramm erlaubt.

- Die Funktion zur Benachrichtigung des Benutzers (s. Pkt. 15.9.1 auf S. 219) über bestimmte Ereignisse während der Programmarbeit wurde erweitert. Für jeden Ereignistyp kann eine Benachrichtigungsmethode festgelegt werden: E-Mail-Nachricht, Audiosignal, Popup-Meldung, Eintrag im Ereignisbericht.

- Eine Technologie zum Selbstschutz der Anwendung, zum Schutz vor unerlaubter Fernsteuerung des Diensts Kaspersky Anti-Virus sowie zum

Kennwortschutz für den Zugriff auf die Anwendungseinstellungen wurde hinzugefügt. Dadurch kann verhindert werden, dass schädliche Programme, Angreifer oder unqualifizierte Benutzer den Schutz ausschalten.

- Eine Option zum Erstellen einer Notfall-CD für die Systemwiederherstellung wurde hinzugefügt. Mit Hilfe dieser CD/DVD lässt sich nach einem Virenangriff das Betriebssystem laden und der Computer kann auf die Existenz schädlicher Objekte untersucht werden.
- Der News Agent wurde hinzugefügt. Dabei handelt es sich um ein Modul, das der schnellen Zustellung der Neuigkeiten von Kaspersky Lab dient.

Neuerungen auf der Programmoberfläche

- Auf der neuen Oberfläche von Kaspersky Anti-Virus ist der einfache und komfortable Zugriff auf alle Programmfunktionen realisiert. Außerdem lässt sich das Programmdesign durch die Verwendung eigener grafischer Elemente und Farbschemen anpassen.
- Bei der Arbeit mit dem Programm werden Sie vollständig mit Informationen unterstützt: Kaspersky Anti-Virus zeigt Meldungen über den Schutzstatus an und besitzt ein ausführliches Hilfesystem. Der im Lieferumfang der Anwendung enthaltene Sicherheitsassistent erlaubt es, ein vollständiges Bild über den aktuellen Zustand des Computerschutzes zu erhalten und Probleme sofort zu beheben.

Neuerungen beim Programm-Update

- In dieser Anwendungsversion wurde eine optimierte Updateprozedur realisiert: Kaspersky Anti-Virus kontrolliert nun automatisch, ob an der Updatequelle ein neues Updatepaket vorhanden ist. Wenn neue Updates gefunden werden, lädt die Anwendung sie herunter und installiert sie auf dem Computer.
- Nur fehlende Updates werden heruntergeladen. Dadurch lässt sich das Volumen des beim Update notwendigen Netzwerkverkehrs bis um das Zehnfache verringern.
- Die Aktualisierung erfolgt von der effektivsten Updatequelle.
- Es besteht die Möglichkeit, keinen Proxyserver zu verwenden, wenn das Programm-Update über eine lokale Quelle erfolgt. Dadurch wird das Volumen des Netzwerkverkehrs über den Proxyserver erheblich vermindert.
- Eine Option zum Rollback von Updates wurde realisiert. Dadurch wird beispielsweise bei einer Beschädigung von Dateien oder bei einem Kopierfehler erlaubt, zur vorherigen Version der Programm-Datenbanken zurückzukehren.

- Eine Option zum Verwenden eines Diensts für die Update-Verteilung in einen lokalen Ordner wurde hinzugefügt. Wird anderen Netzwerkcomputern Zugriff auf den Ordner gewährt, dann lässt sich Internet-Datenverkehr einsparen.

2.2. Die Schutzprinzipien von Kaspersky Anti-Virus

Der Schutz von Kaspersky Anti-Virus wird von den Bedrohungsquellen ausgehend aufgebaut. Für jede Quelle ist eine separate Programmkomponente vorgesehen, die ihre Kontrolle und notwendige Maßnahmen zur Verhinderung schädlicher Einwirkungen dieser Quelle auf die Benutzerdaten gewährleistet. Diese Konzeption des Schutzsystems erlaubt es, die Anwendung flexibel einzusetzen und den Erfordernissen eines konkreten Benutzers oder Unternehmens anzupassen.

Kaspersky Anti-Virus umfasst:

- Echtzeitschutz-Komponenten (s. Pkt. 2.2.1 auf S. 23), die den Echtzeitschutz Ihres Computers auf allen Kanälen gewährleisten, auf denen Daten empfangen und übertragen werden.
- Aufgaben zur Virensuche (s. Pkt. 2.2.2 auf S. 25), mit deren Hilfe die Virenuntersuchung in einzelnen Dateien, Ordnern, Laufwerken oder Bereichen, oder die vollständige Untersuchung des Computers ausgeführt wird.
- Update (s. Pkt. 2.2.3 auf S. 25), das die Aktualität der internen Programm-Module sowie der Datenbanken, die der Suche nach schädlichen Programmen, dem Erkennen von Hackerangriffen und Spam-Mails dienen, gewährleistet.
- Servicefunktionen (s. Pkt. 2.2.4 auf S. 26), die Informationen über die Arbeit mit dem Programm bieten und es erlauben, die Programmfunktionalität zu erweitern.

2.2.1. Echtzeitschutz-Komponenten

Der Echtzeitschutz Ihres Computers wird durch folgende Schutzkomponenten gewährleistet:

Datei-Anti-Virus

Das Dateisystem kann Viren und andere gefährliche Programme enthalten. Nachdem Schadprogramme über einen Wechseldatenträger oder das Inter-

net eingedrungen sind, können sie sich jahrelang im Dateisystem des Computers befinden, ohne dass ihre Existenz bemerkt wird. Sobald eine infizierte Datei aber geöffnet wird, kann der Virus aktiv werden.

Datei-Anti-Virus ist eine Komponente, die das Dateisystem des Computers kontrolliert. Er untersucht auf Ihrem Computer und auf allen angeschlossenen Laufwerken alle Dateien, die geöffnet, gestartet und gespeichert werden. Jeder Zugriff auf eine Datei wird von der Anwendung abgefangen und die Datei wird auf die Existenz bekannter Viren untersucht. Die weitere Arbeit mit der Datei ist nur dann möglich, wenn die Datei virenfrei ist oder erfolgreich von Anti-Virus desinfiziert wurde. Wenn die Desinfektion der Datei aus bestimmten Gründen nicht möglich ist, wird sie gelöscht, wobei eine Kopie der Datei im Backup (s. Pkt. 15.2 auf S. 193) abgelegt oder in der Quarantäne (s. Pkt. 15.1 auf S. 188) gespeichert wird.

Mail-Anti-Virus

Die E-Mail-Korrespondenz wird von Angreifern häufig zur Verbreitung schädlicher Programme verwendet. Sie ist eines der wichtigsten Medien zur Verbreitung von Würmern. Deshalb ist es äußerst wichtig, alle E-Mail-Nachrichten zu kontrollieren.

Mail-Anti-Virus ist eine Komponente zur Untersuchung aller ein- und ausgehenden E-Mail-Nachrichten Ihres Computers. Sie analysiert E-Mails auf Schadprogramme. Eine E-Mail wird nur dann zugestellt, wenn sie keine gefährlichen Objekte enthält.

Web-Anti-Virus

Wenn Sie im Internet bestimmte Webseiten öffnen, riskieren Sie, dass Ihr Computer durch Viren infiziert wird, die mit Hilfe von auf Webseiten enthaltenen Skripts auf dem Computer installiert werden. Außerdem kann ein gefährliches Objekt auf Ihren Computer geladen werden.

Web-Anti-Virus wurde speziell zur Verhinderung solcher Situationen entwickelt. Skripts, die sich auf Webseiten befinden und gefährlich sind, werden von dieser Komponente abgefangen und ihre Ausführung wird gesperrt. Auch der HTTP-Verkehr unterliegt einer strengen Kontrolle.

Proaktiver Schutz

Die Zahl der schädlichen Programme nimmt jeden Tag zu. Malware wird komplizierter, mehrere Arten werden miteinander kombiniert, ihre Ausbreitungsmethoden verändern sich und sie sind immer schwieriger zu erkennen.

Um ein neues Schadprogramm zu erkennen, bevor es Schaden anrichten kann, hat Kaspersky Lab eine spezielle Komponente entwickelt: Den *Proaktiven Schutz*. Er basiert auf der Kontrolle und Analyse des Verhaltens aller Programme, die auf Ihrem Computer installiert sind. Aufgrund der auszuführenden Aktionen entscheidet Kaspersky Anti-Virus, ob ein Programm poten-

tiell gefährlich ist oder nicht. So ist Ihr Computer nicht nur vor bekannten Viren, sondern auch vor neuen, bisher unbekannten Viren geschützt.

2.2.2. Aufgaben zur Virensuche

Neben dem Echtzeitschutz aller Quellen, aus denen Schadprogramme eindringen können, ist es sehr wichtig, regelmäßig die vollständige Virenuntersuchung Ihres Computers durchzuführen. Das ist erforderlich, um die Möglichkeit der Ausbreitung schädlicher Programme auszuschließen, die nicht von den Echtzeitschutz-Komponenten erkannt wurden, weil beispielsweise eine zu niedrige Schutzstufe eingestellt war oder aus anderen Gründen.

Kaspersky Anti-Virus verfügt über folgende Aufgaben zur Virensuche:

Kritische Bereiche

Dazu zählen: Systemspeicher, Objekte, die beim Systemstart ausgeführt werden, Laufwerksbootsektoren und die Systemverzeichnisse von *Microsoft Windows*. Das Ziel dieser Aufgaben besteht darin, aktive Viren im System schnell zu erkennen, ohne den Computer vollständig zu untersuchen.

Arbeitsplatz

Virensuche auf Ihrem Computer mit sorgfältiger Untersuchung aller angeschlossenen Laufwerke, des Arbeitsspeichers und der Dateien.

Autostart-Objekte

Virenuntersuchung der Objekte, die beim Start des Betriebssystems geladen werden, sowie des Arbeitsspeichers und der Laufwerksbootsektoren.

Suche nach Rootkits

Im Computer wird nach Rootkits gesucht, die schädliche Programme im Betriebssystem verstecken. Diese Utilities dringen ins System ein und tarnen ihre eigene Existenz sowie die Existenz von in der Konfiguration des Rootkits beschriebener Malware, die sich in Prozessen, Ordnern oder Registrierungsschlüsseln des Systems befinden kann.

Außerdem besteht die Möglichkeit, andere Untersuchungsaufgaben zu erstellen und Zeitplan für ihren Start anzulegen. Es kann beispielsweise eine Aufgabe zur wöchentlichen Untersuchung von Mailboxen oder eine Aufgabe zur Virensuche im Ordner **Eigene Dateien** erstellt werden.

2.2.3. Update

Um stets bereit zu sein, Hackerangriffe abzuwehren und Viren oder andere gefährliche Programme zu neutralisieren, ist es erforderlich, den aktuellen Zustand

von Kaspersky Anti-Virus zu gewährleisten. Dazu dient die Komponente *Update*. Sie ist für die Aktualisierung der Datenbanken und Programm-Module verantwortlich, die bei der Arbeit von Kaspersky Anti-Virus verwendet werden.

Der Dienst zur Update-Verteilung erlaubt es, die Updates für die Datenbanken und für die Programm-Module, die von den Kaspersky-Lab-Updateservern heruntergeladen wurden, in einem lokalen Ordner zu speichern. Dieser Ordner kann anderen Computern des Netzwerks als Updatequelle dienen, um Datenverkehr einzusparen.

2.2.4. Servicefunktionen des Programms

Kaspersky Anti-Virus verfügt über eine Reihe von Servicefunktionen. Sie dienen dazu, den aktuellen Zustand des Programms aufrechtzuerhalten, die Optionen des Programms zu erweitern und bei der Arbeit Hilfe zu leisten.

Datenverwaltung

Während der Arbeit der Anwendung wird für jede Schutzkomponente, Untersuchungsaufgabe und Update-Aufgabe der Anwendung ein Bericht erstellt. Er enthält Informationen über die ausgeführten Operationen und die Arbeitsergebnisse. Unter Verwendung der Funktion *Berichte* können Sie stets Details über die Arbeit einer beliebigen Komponente von Kaspersky Anti-Virus erhalten. Sollten Probleme auftreten, dann können Sie die Berichte an Kaspersky Lab schicken, damit unsere Experten die Situation analysieren und Ihnen möglichst schnell helfen können.

Alle im Hinblick auf die Sicherheit verdächtigen Objekte werden von Kaspersky Anti-Virus in den speziellen Speicher *Quarantäne* verschoben. Sie werden dort in verschlüsselter Form gespeichert, um eine Infektion des Computers auszuschließen. Sie können die Quarantäne-Objekte auf Viren untersuchen, am ursprünglichen Ort wiederherstellen oder löschen. Außerdem können Sie verdächtige Objekte manuell in die Quarantäne verschieben. Alle Objekte, die sich aufgrund der Untersuchung als virenfrei erweisen, werden automatisch am ursprünglichen Ort wiederhergestellt.

Im *Backup* werden Kopien von Objekten gespeichert, die von der Anwendung desinfiziert und gelöscht wurden. Diese Kopien werden angelegt, um bei Bedarf die Objekte oder ein Bild ihrer Infektion wiederherzustellen. Auch die Sicherungskopien der Objekte werden in verschlüsselter Form gespeichert, um eine Infektion des Computers auszuschließen. Sie können ein Backup-Objekt am ursprünglichen Ort wiederherstellen oder die Sicherungskopie löschen.

Aktivierung

Beim Kauf von Kaspersky Anti-Virus wird zwischen Ihnen und Kaspersky Lab ein Lizenzvertrag abgeschlossen, auf dessen Grundlage Sie die An-

wendung verwenden dürfen und für einen festgelegten Zeitraum Zugriff auf Updates für die Programm-Datenbanken und auf den Technischen Support-Service erhalten. Die Nutzungsdauer sowie andere Informationen, die für die vollfunktionale Arbeit der Anwendung erforderlich sind, befinden sich in einer Schlüsseldatei.

Durch Verwendung der Funktion *Aktivierung* können Sie ausführliche Informationen über den von Ihnen verwendeten Schlüssel und über den Erwerb eines neuen Schlüssels erhalten.

Support

Alle registrierten Benutzer von Kaspersky Anti-Virus können den technischen Support-Service in Anspruch nehmen. Verwenden Sie die Funktion *Support*, um zu erfahren, wo Sie technische Unterstützung erhalten können.

Mit Hilfe der entsprechenden Links gelangen Sie zum Benutzerforum für die Kaspersky-Lab-Produkte und können auf der Webseite ein spezielles Formular ausfüllen, um eine Fehlermeldung oder eine Rückmeldung über die Arbeit des Programms an den Technischen Support-Service zu senden.

Zusätzlich stehen Ihnen der Online-Service des technischen Kundendiensts und die Dienste für das Personal Cabinet des Benutzers zur Verfügung. Natürlich können Sie sich auch per Telefon oder E-Mail an unsere Mitarbeiter wenden, um Hilfe zu erhalten.

2.3. Hardware- und Softwarevoraussetzungen

Um die normale Funktionsfähigkeit von Kaspersky Anti-Virus 7.0 zu gewährleisten, sind folgende Systemvoraussetzungen zu erfüllen.

Allgemeine Voraussetzungen:

- 50 MB freier Speicher auf der Festplatte
- CD/DVD-ROM-Laufwerk (zur Installation von Kaspersky Anti-Virus 7.0 von CD/DVD-ROM).
- Microsoft Internet Explorer Version 5.5 oder höher (für das Update der Programm-Datenbanken und Programm-Module über das Internet)
- Microsoft Windows Installer 2.0.

Unter Microsoft Windows 2000 Professional (Service Pack 4 oder höher), Microsoft Windows XP Home Edition, Microsoft Windows XP Professional (Service Pack 2 oder höher), Microsoft Windows XP Professional x64 Edition:

- Prozessor Intel Pentium 300 MHz oder höher (oder ein entsprechender kompatibler Prozessor)
- 128 MB Arbeitsspeicher.

Microsoft Windows Vista, Microsoft Windows Vista x64:

- Prozessor Intel Pentium 800 MHz 32-Bit (x86) / 64-Bit (x64) oder höher (oder ein entsprechender kompatibler Prozessor)
- 512 MB Arbeitsspeicher.

2.4. Lieferumfang

Kaspersky Anti-Virus kann bei unseren Vertriebspartnern (als verpackte Variante) oder in einem Online-Shop (z.B. www.kaspersky.com/de, Abschnitt **E-Store**) erworben werden.

Wenn Sie das Produkt als verpackte Variante erwerben, umfasst der Lieferumfang des Softwareprodukts die folgenden Elemente:

- Versiegelter Umschlag mit Installations-CD, auf der die Programmdateien und die Dokumentation im PDF-Format gespeichert sind.
- Benutzerhandbuch in ausgedruckter Form (wenn Position im Auftrag enthalten war) oder Programmführer.
- Code zur Programmaktivierung (auf dem Umschlag mit der Installations-CD aufgeklebt).
- Lizenzvertrag.

Hinweis

Bitte lesen Sie vor der Installation sorgfältig den Lizenzvertrag im Anhang des Handbuchs.

Beim Kauf von Kaspersky Anti-Virus in einem Online-Shop kopieren Sie das Produkt von der Kaspersky-Lab-Webseite (Abschnitt **Downloads → Produkte herunterladen**). Das Benutzerhandbuch kann aus dem Abschnitt **Downloads → Dokumentationen** heruntergeladen werden.

Der Aktivierungscode wird Ihnen nach Eingang der Bezahlung per E-Mail zugeschickt.

Der Lizenzvertrag ist eine rechtsgültige Vereinbarung zwischen Ihnen und Kaspersky Lab Ltd., in der festgelegt wird, zu welchen Bedingungen Sie das von Ihnen erworbene Softwareprodukt verwenden dürfen.

Bitte lesen Sie den Lizenzvertrag sorgfältig!

Durch das Öffnen der versiegelten Packung mit der Installations-CD (oder Disketten) stimmen Sie allen Bedingungen des Lizenzvertrags zu.

2.5. Service für registrierte Benutzer

Kaspersky Lab bietet seinen legalen Benutzern ein breites Spektrum an Serviceleistungen, die eine gesteigerte Effektivität von Kaspersky Anti-Virus ermöglichen.

Durch die Aktivierung des Programms werden Sie zum registrierten Programmbenutzer und können während der Gültigkeitsdauer des Schlüssels folgende Dienste in Anspruch nehmen:

- Nutzung neuer Versionen der betreffenden Software
- Beratung bei Fragen zu Installation, Konfiguration und Benutzung der Software (per Telefon und E-Mail)
- Nachrichten über das Erscheinen neuer Software von Kaspersky Lab und über das Auftauchen neuer Viren (Dieser Service gilt für Benutzer, die den Newsletter von Kaspersky Lab abonniert haben).

Hinweis

Die Beratung bezieht sich nicht auf Fragen über Funktion und Benutzung von Betriebssystemen und anderen Technologien.

KAPITEL 3. INSTALLATION VON KASPERSKY ANTI-VIRUS 7.0

Es bestehen mehrere Möglichkeiten, um Kaspersky Anti-Virus 7.0 auf dem Computer zu installieren:

- interaktiver Modus mit Hilfe des Installationsassistenten für das Programm (s. Pkt. 3.1 auf S. 30). In diesem Modus sind während der Installation bestimmte Aktionen des Benutzers erforderlich.
- Silent-Modus. In diesem Fall wird die Programminstallation aus der Befehlszeile gestartet und erfordert während des Installationsvorgangs keine weiteren Aktionen des Benutzers (s. Pkt. 3.3 auf S. 43).

Achtung!

Es wird empfohlen, alle laufenden Anwendungen zu beenden, bevor mit der Installation von Kaspersky Anti-Virus begonnen wird.

3.1. Installation mit Hilfe des Assistenten

Hinweis

Die Installation der Anwendung von einer Distribution, die aus dem Internet heruntergeladen wurde, stimmt vollständig mit der Installation der Anwendung von einer Distributions-CD überein.

Um Kaspersky Anti-Virus auf Ihrem Computer zu installieren, starten Sie die Distributionsdatei (Datei mit der Endung **.exe*) von der Produkt-CD.

Daraufhin erfolgt die Suche nach dem Installationspaket für die Anwendung (Datei mit der Endung **.msi*). Wenn das Paket vorhanden ist, wird Ihnen angeboten, zu prüfen, ob auf den Kaspersky-Lab-Servern im Internet eine neuere Version von Kaspersky Anti-Virus vorhanden ist. Wird die Datei mit dem Installationspaket nicht gefunden, dann wird Ihnen angeboten, sie herunterzuladen. Nach dem Download wird die Programminstallation gestartet.

Bei Ablehnung des Downloads wird die Programm im normalen Modus fortgesetzt.

Das Installationsprogramm funktioniert im Dialogmodus. Jedes Dialogfenster enthält eine Auswahl von Schaltflächen zur Steuerung des Installationsprozesses. Unten finden Sie die Funktionsbeschreibung der wichtigsten Schaltflächen:

- **Weiter** – Aktion bestätigen und zum folgenden Schritt des Installationsvorgangs weitergehen.
- **Zurück** – zum vorherigen Installationsschritt zurückkehren.
- **Abbrechen** – Installation des Produkts abbrechen.
- **Fertig stellen** – Installationsprozedur des Programms auf dem Computer fertig stellen.

Betrachten wir die einzelnen Schritte des Installationsvorgangs ausführlich:

Schritt 1. Überprüfen des Systems auf die Installationsvoraussetzungen für Kaspersky Anti-Virus

Bevor das Programm auf Ihrem Computer installiert wird, werden das installierte Betriebssystem und die vorhandenen Service Packs auf Übereinstimmung mit den Softwarevoraussetzungen für die Installation von Kaspersky Anti-Virus überprüft. Außerdem wird überprüft, ob die erforderlichen Programme auf Ihrem Computer vorhanden sind und ob Sie über die notwendigen Rechte zur Programminstallation verfügen.

Sollte eine bestimmte Voraussetzung nicht erfüllt sein, dann erscheint eine entsprechende Meldung auf dem Bildschirm. Es wird empfohlen, vor der Installation von Kaspersky Anti-Virus die erforderlichen Programme und mit Hilfe des Diensts **Windows Update** die fehlenden Service Packs zu installieren.

Schritt 2. Startfenster des Installationsvorgangs

Wenn Ihr System die Voraussetzungen vollständig erfüllt, erscheint sofort nach dem Start der Distributionsdatei auf dem Bildschirm das Startfenster, das Informationen über den Beginn der Installation von Kaspersky Anti-Virus auf Ihrem Computer enthält.

Klicken Sie auf **Weiter**, um die Installation fortzusetzen, oder klicken Sie auf **Abbrechen**, um die Installation des Produkts zu abzubrechen.

Schritt 3. Lesen des Lizenzvertrags

Das folgende Fenster des Installationsprogramms enthält den Lizenzvertragg, der zwischen Ihnen und Kaspersky Lab geschlossen wird.. Bitte lesen Sie den

Vertrag aufmerksam. Wenn Sie allen Punkten des Vertrags zustimmen, wählen Sie die Variante **Ich akzeptiere die Bedingungen des Lizenzvertrags** und klicken Sie auf die Schaltfläche **Weiter**. Die Installation wird fortgesetzt.

Schritt 4. Auswahl des Installationstyps

Auf dieser Etappe können Sie die geeignete Methode für die Installation der Anwendung wählen:

Schnelle Installation. Bei Auswahl dieser Variante wird Kaspersky Anti-Virus vollständig mit den von Kaspersky Labs Spezialisten empfohlenen Einstellungen auf Ihrem Computer installiert. Am Ende der Installation wird der Aktivierungsassistent der Anwendung gestartet (s. Pkt. 3.2.2 auf S. 36).

Benutzerdefinierte Installation. In diesem Fall können Sie die Programmkomponenten wählen, die auf dem Computer installiert werden soll und den Installationsordner festlegen. Außerdem können Sie mit Hilfe eines speziellen Assistenten die Anwendung aktivieren und vorab konfigurieren (s. Pkt. 3.2 auf S. 35).

Bei Auswahl der ersten Variante verläuft die Installation ohne Interaktion mit dem Benutzer, d.h. alle in diesem Abschnitt genannten Schritte werden übersprungen. Im zweiten Fall ist auf jeder Installationsetappe die Eingabe oder Bestätigung bestimmter Daten durch den Benutzer erforderlich.

Schritt 5. Auswahl des Installationsordners

Im nächsten Schritt der Installation von Kaspersky Anti-Virus wird festgelegt, in welchem Ordner Ihres Computers das Produkt installiert werden soll. Der standardmäßige Pfad lautet:

- **<Laufwerk> → Programme → Kaspersky Lab → Kaspersky Anti-Virus 7.0** – für 32-Bit-Systeme
- **<Laufwerk> → Programme (x86) → Kaspersky Lab → Kaspersky Anti-Virus 7.0** – für 64-Bit-Systeme

Sie können einen anderen Ordner wählen. Klicken Sie dazu auf die Schaltfläche **Durchsuchen** und wählen Sie den Ordner im Standardfenster zur Ordnerauswahl aus oder geben Sie den Pfad des Ordners im entsprechenden Eingabefeld an.

Achtung!

Falls Sie den vollständigen Pfad des Ordners manuell angeben, beachten Sie, dass er aus maximal 200 Zeichen bestehen und keine Sonderzeichen enthalten

darf.

Klicken Sie auf die Schaltfläche **Weiter**, um die Installation fortzusetzen.

Schritt 6. Auswahl der zu installierenden Programmkomponenten

Hinweis

Dieser Schritt wird nur bei der **benutzerdefinierten** Installation des Programms ausgeführt.

Bei der benutzerdefinierten Installation muss eine Liste der Komponenten von Kaspersky Anti-Virus festgelegt werden, die installiert werden sollen. Standardmäßig sind alle Echtzeitschutz-Komponenten zur Virensuche gewählt.

Um eine Komponente zur anschließenden Installation auszuwählen, wird durch Linksklick auf das Symbol neben dem Komponentennamen das Menü geöffnet und der Punkt **Die Komponente wird auf der lokalen Festplatte installiert** gewählt. Eine Beschreibung des Schutzes, den die betreffende Komponente gewährleistet und Informationen über den für ihre Installation auf der Festplatte erforderlichen Platz befinden sich im unteren Bereich dieses Fensters der Programminstallation.

Um die Installation einer Komponente abzulehnen, wählen Sie im Kontextmenü die Variante **Die Komponente wird nicht verfügbar sein**. Beachten Sie, dass Sie auf den Schutz vor einer ganzen Reihe gefährlicher Programme verzichten, wenn Sie eine bestimmte Komponente nicht installieren.

Klicken Sie auf die Schaltfläche **Weiter**, nachdem Sie die zu installierenden Komponenten gewählt haben. Um zur Liste der standardmäßig zu installierenden Komponenten zurückzukehren, klicken Sie auf die Schaltfläche **Zurücksetzen**.

Schritt 7. Verwendung von Programmparametern, die von der vorherigen Installation gespeichert wurden

Auf dieser Etappe können Sie festlegen, ob bei der Arbeit des Programms die Schutzeinstellungen und Programm-Datenbanken verwendet werden sollen, wenn solche auf Ihrem Computer bei der Deinstallation einer älteren Version von Kaspersky Anti-Virus gespeichert wurden.

Im Folgenden wird beschrieben, wie die Verwendung der oben genannten Optionen aktiviert wird.

Wenn auf Ihrem Computer bereits eine ältere Version von Kaspersky Anti-Virus installiert war und bei der Deinstallation die Programm-Datenbanken auf dem Computer gespeichert wurden, können Sie diese in der zu installierenden Versi-

on verwenden. Aktivieren Sie dazu das Kontrollkästchen **Programm-Datenbanken**. Die Datenbanken, die in der Programmdistribution enthalten sind, werden dann nicht auf Ihren Computer kopiert.

Um die Schutzparameter zu verwenden, die Sie in der vorherigen Version eingestellt und auf dem Computer gespeichert haben, aktivieren Sie das Kontrollkästchen **Schutzeinstellungen**.

Schritt 8. Suche anderer Antiviren-Programme

Auf dieser Etappe erfolgt die Suche nach anderen Antiviren-Produkten (einschließlich Kaspersky-Lab-Produkte), die auf Ihrem Computer installiert sind und deren gemeinsame Verwendung mit Kaspersky Anti-Virus zu Konflikten führen kann.

Wenn auf Ihrem Computer solche Programme gefunden werden, werden Sie auf dem Bildschirm aufgelistet. Sie werden aufgefordert, diese Programme zu löschen, bevor die Installation fortgesetzt wird.

Unter der Liste der gefundenen Antiviren-Anwendungen können Sie wählen, ob diese automatisch oder manuell entfernt werden sollen.

Wenn sich Kaspersky Anti-Virus 6.0 unter den gefundenen Antiviren-Programmen befindet, wird bei manueller Deinstallation empfohlen, díe für die Arbeit des Programms verwendete Schlüsseldatei zu speichern.. Sie können ihn als Schlüssel für Kaspersky Anti-Virus 7.0 verwenden. Außerdem wird empfohlen, die Quarantäne- und Backup-Objekte zu speichern. Diese Objekte werden automatisch in die entsprechenden Speicher von Kaspersky Anti-Virus verschoben und Sie können damit weiterarbeiten.

Bei der automatischen Deinstallation von Kaspersky Anti-Virus 6.0 werden die Aktivierungsdaten vom Programm gespeichert und bei der Installation von Version 7.0 automatisch übernommen.

Klicken Sie auf die Schaltfläche **Weiter**, um die Installation fortzusetzen.

Achtung!

Kaspersky Anti-Virus 7.0 unterstützt Schlüsseldateien für Version 6.0 und 7.0. Schlüssel, die für Programme der Version 5.0 dienen, werden nicht unterstützt.

Schritt 9. Abschlussvorbereitungen für die Programminstallation

Nun wird Ihnen angeboten, die Programminstallation auf Ihrem Computer abschließend vorzubereiten.

Bei der Erstinstallation von Kaspersky Anti-Virus 7.0 sollte das Kontrollkästchen **Schutz für Module vor der Installation aktivieren** nicht entfernt werden.

Der aktivierte Modulschutz erlaubt, falls während der Anwendungsinstallation Fehler auftreten, die Installation auf korrekte Weise rückgängig zu machen. Bei einem wiederholten Versuch zur Installation der Anwendung wird empfohlen, dieses Kontrollkästchen zu entfernen.

Hinweis

Wird die Anwendung im entfernten Modus über **Windows Remote Desktop** auf dem Computer installiert, dann wird empfohlen, das Kontrollkästchen ☑ **Schutz für Module vor der Installation aktivieren** zu deaktivieren. Andernfalls besteht die Möglichkeit, dass der Installationsvorgang nicht oder fehlerhaft durchgeführt wird.

Klicken Sie auf die Schaltfläche **Weiter**, um die Installation fortzusetzen.

Achtung!

Während Komponenten von Kaspersky Anti-Virus installiert werden, die der Kontrolle des Netzwerkverkehrs dienen, werden bestehende Netzwerkverbindungen getrennt. Die Mehrzahl der getrennten Verbindungen wird nach einiger Zeit wieder hergestellt.

Schritt 10. Abschluss des Installationsvorgangs

Das Fenster **Installation wird abgeschlossen** enthält Informationen über den Abschluss des Installationsprozesses von Kaspersky Anti-Virus auf Ihrem Computer.

Wenn zum Fertigstellen der Programminstallation der Neustart des Computers erforderlich ist, erscheint eine entsprechende Meldung auf dem Bildschirm. Nach dem Neustart des Systems wird automatisch der Konfigurationsassistent für Kaspersky Anti-Virus gestartet.

Wenn zum Fertigstellen der Installation kein Systemneustart erforderlich ist, klicken Sie auf die Schaltfläche **Weiter**, um zum Konfigurationsassistenten des Programms zu wechseln.

3.2. Konfigurationsassistent

Der Konfigurationsassistent für Kaspersky Anti-Virus 7.0 wird beim Abschluss der Programminstallation gestartet. Seine Aufgabe ist es, Sie bei der ersten Konfiguration der Programmeinstellungen zu unterstützen und dabei die Besonderheiten der Aufgaben Ihres Computers zu berücksichtigen.

Der Konfigurationsassistent besitzt das Aussehen eines Microsoft Windows-Programmassistenten (Windows Wizard) und besteht aus einer Folge von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Weiter** und **Zurück**, zum Abschluss des Assistenten klicken Sie auf die Schaltfläche **Fertig stellen**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf die Schaltfläche **Abbrechen** beendet werden.

Sie können die Etappen des Konfigurationsassistenten bei der Programminstallation überspringen, indem Sie das Assistentenfenster schließen. Der Assistent kann später über die Programmoberfläche gestartet werden, wenn die ursprünglichen Schutzeinstellungen von Kaspersky Anti-Virus wiederhergestellt werden (s. Pkt. 15.9.4 auf S. 227).

3.2.1. Verwendung von Objekten, die in Version 5.0 gespeichert wurden

Dieses Fenster des Assistenten erscheint, wenn die Anwendung über Kaspersky Anti-Virus Version 5.0 installiert wird. Ihnen wird angeboten, die Daten, die von Version 5.0 verwendet wurden und auf Version 7.0 übertragen werden sollen, auszuwählen. Dazu gehören Quarantäne- und Backup-Objekte sowie Schutzeinstellungen.

Aktivieren Sie die entsprechenden Kontrollkästchen, um diese Daten in Version 7.0 zu verwenden.

3.2.2. Aktivierung des Programms

Hinweis

Vergewissern Sie sich, dass das Systemdatum des Computers korrekt eingestellt ist, bevor Sie das Programm aktivieren.

Der Aktivierungsvorgang des Programms besteht in der Installation eines Schlüssels, auf dessen Grundlage Kaspersky Anti-Virus ermittelt, ob Rechte für die Programmnutzung bestehen und welche Nutzungsdauer vorliegt.

Der Schlüssel enthält Dienstinformationen, die für die volle Funktionsfähigkeit des Programms erforderlich sind, sowie zusätzliche Angaben:

- Informationen über den Support (von wem und wo man technische Unterstützung erhalten kann).
- Bezeichnung, Nummer und Gültigkeitsende des Schlüssels.

3.2.2.1. Auswahl der Aktivierungsmethode

Abhängig davon, ob Sie über einen Schlüssel für das Programm Kaspersky Anti-Virus verfügen oder ihn von einem Kaspersky-Lab-Server erhalten müssen, bestehen mehrere Möglichkeiten zur Aktivierung des Programms:

- **Mit Aktivierungscode aktivieren**. Wählen Sie diese Aktivierungsmethode, wenn Sie eine kommerzielle Programmversion erworben haben und Sie einen Aktivierungscode erhalten haben. Auf Basis dieses Codes bekommen Sie eine Schlüsseldatei, die Ihnen während der gesamten Gültigkeitsdauer des Lizenzvertrags den Zugriff auf die volle Funktionsfähigkeit des Programms bietet.
- **Testversion aktivieren**. Wählen Sie diese Aktivierungsvariante, wenn Sie eine Testversion des Programms installieren möchten, bevor Sie über den Kauf einer kommerziellen Version entscheiden. Sie erhalten einen kostenlosen Schlüssel, dessen Gültigkeitsdauer durch den Lizenzvertrag der Testversion dieser Anwendung beschränkt ist.
- **Vorhandenen Schlüssel verwenden**. Aktivieren Sie die Anwendung mit Hilfe einer bereits vorhandenen Schlüsseldatei für Kaspersky Anti-Virus 7.0.
- **Das Programm später aktivieren**. Bei der Auswahl dieser Variante wird die Aktivierung des Programms übersprungen. Kaspersky Anti-Virus 7.0 wird auf Ihrem Computer installiert und Sie können alle Programmfunktionen außer dem Update nutzen (Das Programm kann nach der Installation nur einmal aktualisiert werden).

Achtung!

Wenn zur Programmaktivierung eine der ersten beiden Varianten gewählt wird, ist eine Internetverbindung notwendig. Ist im Augenblick der Installation keine Internetverbindung vorhanden, dann kann die Aktivierung später über die Programmoberfläche erfolgen (s. Kapitel 14 auf S. 185). Außerdem besteht auch die Möglichkeit, von einem anderen Computer aus ins Internet zu gehen, sich auf der Webseite des Technischen Support-Services von Kaspersky Lab anzumelden und mit Hilfe des Aktivierungscodes einen Schlüssel herunterzuladen.

3.2.2.2. Eingabe des Aktivierungscodes

Zur Aktivierung des Programms ist die Eingabe des Aktivierungscodes erforderlich, den Sie auf der beiliegenden Registrierungskarte finden. Der Code muss mit lateinischen Zeichen eingegeben werden

Der Aktivierungscode besteht aus einer durch Bindestriche getrennten Folge von Ziffern und Buchstaben (vier Blöcke zu je fünf Zeichen ohne Leerzeichen, z.B.

11AA1-11AAA-1AA11-1A111). Bitte beachten Sie, dass der Code mit lateinischen Zeichen eingegeben werden muss.

Wenn Sie den Registriervorgang für Kunden von Kaspersky Lab auf der Webseite des Technischen Kundendienstes schon absolviert haben und Sie eine Kundennummer und ein Kundenkennwort haben, aktivieren Sie das Kontrollkästchen **Ich habe bereits eine Kundennummer** und tragen Sie diese Daten im unteren Fensterteil ein.

Wenn Sie sich noch nicht registriert haben, klicken Sie auf die Schaltfläche **Weiter**, ohne das Kontrollkästchen zu aktivieren. Geben Sie im unteren Bereich des Fensters Ihre Kundennummer und Ihr Kennwort ein, wenn Sie bereits als Kunde bei Kaspersky Lab registriert sind. Falls sich noch nicht registriert haben, lassen Sie die Felder leer. In diesem Fall fragt der Aktivierungsassistent auf der nächsten Etappe nach Ihren Kontaktinformationen und führt die Registrierung durch. Zum Abschluss der Registrierung erhalten Sie eine Kundennummer und ein Kennwort, die für die Inanspruchnahme des technischen Supports obligatorisch sind. Bei der Registrierung über den Aktivierungsassistenten wird die Kundennummer im Abschnitt **Support** des Programmhauptfensters angezeigt (s. Pkt. 15.10 auf S. 228).

3.2.2.3. Registrierung des Benutzers

Bei diesem Schritt des Aktivierungsassistenten werden Sie gebeten, Ihre Kontaktinformationen anzugeben: E-Mail-Adresse, Wohnort und Land. Diese Informationen benötigt der Technische Support-Service von Kaspersky Lab um Sie als registrierten Benutzer zu identifizieren.

Der Aktivierungsassistent schickt Ihre Daten an den Aktivierungsserver, von dem Sie dann eine Kundennummer und ein Kennwort für Ihr Personal Cabinet auf der Webseite des Technischen Support-Services erhalten. Informationen zur Kundennummer werden im Abschnitt **Support** des Programmhauptfensters angezeigt .

3.2.2.4. Download der Schlüsseldatei

Der Konfigurationsassistent baut eine Verbindung mit den Kaspersky-Lab-Servern im Internet auf und sendet Ihre Anmeldungsdaten (Aktivierungscode, Kontaktinformationen) zur Überprüfung an den Server.

Bei erfolgreicher Überprüfung des Aktivierungscodes erhält der Assistent eine Schlüsseldatei. Wenn Sie eine Testversion des Programms installieren, erhält der Konfigurationsassistent ohne Aktivierungscode einen Testschlüssel.

Die empfangene Datei wird automatisch für die Arbeit mit dem Programm installiert und das letzte Fenster des Assistenten mit ausführlichen Informationen über den verwendeten Schlüssel wird geöffnet.

Hinweis

Wenn die Aktivierung auf diese Weise erfolgt, erhält das Programm keine echte Datei mit der Endung **.key* vom Server, sondern bestimmte Daten, die in die Registrierung des Betriebssystems und in das Dateisystem eingetragen werden.

Zum Download einer echten Schlüsseldatei ist die Anmeldung des Benutzers auf der Kaspersky-Lab-Webseite erforderlich.

Wenn der Aktivierungscode die Überprüfung nicht besteht, erscheint ein entsprechender Hinweis auf dem Bildschirm. Wenden Sie sich in diesem Fall an die Firma, bei der Sie das Programm erworben haben.

3.2.2.5. Auswahl einer Schlüsseldatei

Wenn Sie bereits eine Schlüsseldatei für das Programm Kaspersky Anti-Virus 7.0 besitzen, bietet Ihnen der Assistent in diesem Fenster an, den Schlüssel zu installieren. Verwenden Sie dazu die Schaltfläche **Durchsuchen** und wählen Sie im Standardfenster zur Dateiauswahl eine Datei mit der Endung *.key* aus.

Nach der erfolgreichen Installation des Schlüssels erscheinen im unteren Bereich des Fensters Informationen über den verwendeten Schlüssel: Name des Besitzers, Nummer und Typ (kommerzieller, für Beta-Test, Test usw.) des Schlüssels, Gültigkeitsdatum des Schlüssels.

3.2.2.6. Abschluss der Programmaktivierung

Der Konfigurationsassistent informiert Sie über den erfolgreichen Abschluss der Programmaktivierung. Außerdem werden Informationen über den installierten Schlüssel angezeigt: Name des Besitzers, Nummer und Typ (kommerzieller, für Beta-Test, Test usw.) des Schlüssels, Gültigkeitsdatum des Schlüssels.

3.2.3. Auswahl des Schutzmodus

In diesem Fenster des Konfigurationsassistenten wird Ihnen angeboten, den Schutzmodus zu wählen, in dem die Anwendung arbeiten soll:

Basisschutz. Dieser Modus gilt als Standard und ist für die meisten Benutzer geeignet, die über begrenzte Erfahrung mit Computern und Antiviren-Produkten verfügen. In diesem Modus funktionieren die Anwendungskom-

ponenten auf der empfohlenen Sicherheitsstufe und der Benutzer wird nur über das Eintreten gefährlicher Ereignisse (z.B. Fund eines schädlichen Objekts, Ausführen gefährlicher Aktionen) informiert.

Interaktiver Schutz. Dieser Modus bietet im Vergleich zum Basisschutz einen erweiterten Schutz für die Daten auf dem Computer. Er erlaubt die Kontrolle über Versuche zum Verändern von Systemeinstellungen und über verdächtige Aktivität im System.

Alle oben genannten Aktionen können sowohl das Ergebnis der Aktivität schädlicher Programme, als auch standardmäßige Aktionen im Rahmen der Arbeit von auf Ihrem Computer verwendeten Programmen sein. Sie müssen in jedem konkreten Fall entscheiden, ob eine Aktion erlaubt oder unzulässig ist.

Wenn Sie diesen Modus wählen, dann geben Sie an, in welchen Fällen er verwendet werden soll:

- **Überwachung der Systemregistrierung aktivieren** – Bei Versuchen zum Ändern von Systemregistrierungsobjekten erfolgt eine Bestätigungsabfrage.

  Achtung!

  Wenn die Anwendung auf einem Computer mit dem Betriebssystem Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista oder Microsoft Windows Vista x64 installiert ist, sind die unten genannten Parameter für den interaktiven Modus nicht vorhanden.

- **Integritätskontrolle für Anwendungen aktivieren** – Wenn versucht wird, Module in die zu kontrollierenden Anwendungen zu laden, erfolgt eine Bestätigungsabfrage.

- **Den erweiterten Proaktiven Schutz aktivieren** – Die Analyse aller verdächtigen Aktivitäten von Anwendungen im System wird aktiviert. Dazu zählen auch Browserstart mit Befehlzeilenschlüsseln, Eindringen in Programmprozesse und Eindringen von Fenster-Hooks (diese Parameter sind standardmäßig deaktiviert).

3.2.4. Konfiguration der Update-Einstellungen

Die Qualität des Schutzes Ihres Computers ist direkt vom rechtzeitigen Download der Updates für die Datenbanken und Programm-Module abhängig. In diesem Fenster des Assistenten wird Ihnen angeboten, den Modus für das Programm-Update zu wählen und Einstellungen für den Zeitplan vorzunehmen:

- **Automatisch**. Kaspersky Anti-Virus prüft in festgelegten Zeitabständen, ob an der Updatequelle ein neues Updatepaket vorhanden ist. Die Häufigkeit der Überprüfung kann während Virusepidemien steigen und unter gewöhnlichen Umständen sinken. Wenn neue Updates vorhanden sind, lädt die Anwendung sie herunter und installiert sie auf dem Computer. Dieser Modus gilt als Standard.
- **Alle 1 Tage** (Das Intervall kann in Abhängigkeit von den Zeitplaneinstellungen variieren). Das Update wird automatisch nach dem festgelegten Zeitplan gestartet. Der Zeitplan wird in dem Fenster angepasst, das durch Klick auf die Schaltfläche **Ändern** geöffnet wird.
- **Manuell**. In diesem Fall starten Sie das Programm-Update selbständig.

Beachten Sie, dass die Datenbanken und die Programm-Module, die in der Distribution enthalten sind, zum Zeitpunkt der Programminstallation bereits veraltet sein können. Wir empfehlen deshalb, die aktuellen Programm-Updates herunterzuladen. Klicken Sie dazu auf die Schaltfläche **Jetzt aktualisieren**. In diesem Fall empfängt Kaspersky Anti-Virus die erforderlichen Updates von den Updateseiten im Internet und installiert sie auf Ihrem Computer.

Wenn Sie die Updateparameter anpassen möchten (die Ressource wählen, von der das Update erfolgt, den am nächsten bei Ihrem Standort liegenden Updateserver festlegen, den Start der Aktualisierung unter einem bestimmten Benutzerkonto konfigurieren, den Dienst zur Update-Verteilung in eine lokale Quelle aktivieren), klicken Sie auf die Schaltfläche **Einstellungen**.

3.2.5. Konfiguration des Zeitplans für die Virenuntersuchung

Die Suche von schädlichen Objekten in vorgegebenen Untersuchungsbereichen ist eine der wichtigsten Aufgaben, die den Schutz Ihres Computers gewährleistet.

Bei der Installation von Kaspersky Anti-Virus werden standardmäßig drei Untersuchungsaufgaben erstellt. In diesem Fenster bietet Ihnen der Assistent an, den Startmodus für die Untersuchungsaufgaben festzulegen:

Autostart-Objekte untersuchen

Standardmäßig findet die Untersuchung der Autostart-Objekte automatisch bei jedem Start von Kaspersky Anti-Virus statt. Die Zeitplaneinstellungen können im Fenster angepasst werden, das mit der Schaltfläche **Ändern** geöffnet wird.

Kritische Bereiche untersuchen

Aktivieren Sie das Kontrollkästchen im entsprechenden Block, damit die Virenuntersuchung der kritischen Computerbereiche (Systemspeicher, Auto-

start-Objekte, Bootsektoren, Microsoft Windows-Systemverzeichnisse) automatisch gestartet wird. Der Zeitplan wird in dem Fenster angepasst, das durch Klick auf die Schaltfläche **Ändern** geöffnet wird.

Der automatische Start dieser Aufgabe ist standardmäßig deaktiviert.

Vollständig Untersuchung des Computers

Aktivieren Sie das Kontrollkästchen im entsprechenden Block, damit die vollständige Untersuchung Ihres Computers auf Viren automatisch gestartet wird. Der Zeitplan wird in dem Fenster angepasst, das durch Klick auf die Schaltfläche **Ändern** geöffnet wird.

Der automatische Start dieser Aufgabe nach Zeitplan ist standardmäßig deaktiviert. Wir empfehlen aber, sofort nach der Programminstallation die vollständige Virenuntersuchung des Computers zu starten.

3.2.6. Zugriffsbegrenzung für die Anwendung

Da ein PC von mehreren Personen benutzt werden kann, die über ein unterschiedliches Maß an Fertigkeiten im Umgang mit Computern verfügen, und weil die Gefahr besteht, dass Schadprogramme versuchen, den Schutz Ihres Computers auszuschalten, bietet Kaspersky Anti-Virus die Möglichkeit, den Zugriff auf die Anwendung mit Hilfe eines Kennworts zu beschränken. Der Kennwortschutz erlaubt es, die Anwendung vor Versuchen zum unerlaubten Abschalten des Schutzes und zum Ändern der Einstellungen zu schützen.

Um den Kennwortschutz zu verwenden, aktivieren Sie das Kontrollkästchen **Kennwortschutz aktivieren** und füllen Sie die Felder **Kennwort** und **Kennwort bestätigen** aus.

Geben Sie darunter den Bereich an, auf den sich die Zugriffsbeschränkung beziehen soll:

- **Alle Operationen (außer Gefahrenmeldungen)**. Bei einer beliebigen Aktion des Benutzers mit der Anwendung wird das Kennwort abgefragt. Eine Ausnahme bildet die Arbeit mit Hinweisen über den Fund gefährlicher Objekte.
- **Nur für ausgewählte Operationen:**
  - **Funktionsparameter der Anwendung ändern** – Wenn der Benutzer versucht, geänderte Anwendungseinstellungen zu speichern, wird das Kennwort abgefragt.
  - **Programm beenden** – Wenn der Benutzer versucht, die Anwendung zu beenden, wird das Kennwort abgefragt.

- **Schutzkomponenten und Untersuchungsaufgaben anhalten/ beenden** – Das Kennwort wird abgefragt, wenn der Benutzer versucht, die Arbeit einer beliebigen Echtzeitschutz-Komponente oder einer Untersuchungsaufgabe anzuhalten oder zu beenden.

3.2.7. Integritätskontrolle für Anwendungen

Auf dieser Etappe des Assistenten analysiert Kaspersky Anti-Virus die auf Ihrem Computer installierten Anwendungen (dynamische Bibliotheksdateien, digitale Herstellersignaturen), berechnet die Kontrollsummen der Anwendungsdateien und erstellt eine Liste der im Hinblick auf die Antiviren-Sicherheit vertrauenswürdigen Programme. In diese Liste werden beispielsweise automatisch alle Anwendungen aufgenommen, die eine Signatur der Microsoft Corporation besitzen.

Die bei der Strukturanalyse der Anwendungen ermittelten Informationen werden danach von der Anwendung Kaspersky Anti-Virus verwendet, um das Eindringen von schädlichem Code in Anwendungsmodule zu verhindern.

Die Analyse der auf Ihrem Computer installierten Anwendungen kann eine gewisse Zeit in Anspruch nehmen.

3.2.8. Abschluss des Konfigurationsassistenten

Im letzten Fenster des Assistenten wird Ihnen angeboten, den Computer neu zu starten, um die Programminstallation fertig zu stellen. Der Neustart ist notwendig, um die Treiber von Kaspersky Anti-Virus korrekt zu registrieren.

Sie können den Neustart des Computers aufschieben. Allerdings werden in diesem Fall bestimmte Schutzkomponenten der Anwendung nicht funktionieren.

3.3. Installation der Anwendung aus der Befehlszeile

Geben Sie zur Installation von Kaspersky Anti-Virus in der Befehlszeile ein:

```
msiexec /i <Paketname>
```

Der Installationsassistent (s. Pkt. 3.1 auf S. 30) wird gestartet. Zum Abschluss der Anwendungsinstallation ist der Neustart des Computers erforderlich.

Um die Anwendung im Silent-Modus (ohne Installationsassistent) zu installieren, geben Sie folgende Befehlszeile ein:

```
msiexec /i <Paketname> /qn
```

KAPITEL 4. PROGRAMM-OBERFLÄCHE

Kaspersky Anti-Virus verfügt über eine einfache und komfortable Oberfläche. In diesem Kapitel werden die wichtigsten Elemente der Oberfläche ausführlich beschrieben:

- Symbol im Infobereich der Taskleiste von Microsoft Windows (s. Pkt. 4.1 auf S. 45)
- Kontextmenü (s. Pkt. 4.2 auf S. 46)
- Hauptfenster (s. Pkt. 4.3 auf S. 48)
- Konfigurationsfenster des Programms (s. Pkt. 4.4 auf S. 53)

Das Programm verfügt außer der Hauptoberfläche noch über Erweiterungskomponenten (Plug-ins), die in folgende Anwendungen integriert werden können:

- Microsoft Outlook (s. Pkt. 8.2.2 auf S. 110)
- The Bat! (s. Pkt. 8.2.3 auf S. 112)
- Microsoft Internet Explorer (s. Kapitel 9 auf S. 119)
- Microsoft Windows Explorer (s. Pkt. 11.2 auf S. 152)

Die Plug-ins erweitern die Möglichkeiten der genannten Programme, da auf ihrer Oberfläche die Steuerung und Konfiguration der entsprechenden Komponenten von Kaspersky Anti-Virus möglich ist.

4.1. Symbol im Infobereich der Taskleiste von Microsoft Windows

Sofort nach der Installation von Kaspersky Anti-Virus erscheint sein Symbol im Infobereich der Taskleiste von Microsoft Windows.

Das Symbol ist ein spezieller Indikator für die Arbeit von Kaspersky Anti-Virus. Er informiert über den Schutzstatus und eine Reihe wichtiger Aufgaben, die vom Programm ausgeführt werden.

Wenn das Symbol aktiv (farbig) ist, ist der Schutz vollständig aktiviert oder bestimmte Schutzkomponenten sind aktiviert. Ist das Symbol inaktiv (schwarz-weiß), dann wurden alle Schutzkomponenten deaktiviert (s. Pkt. 2.2.1 auf S. 23).

Abhängig von der momentan ausgeführten Operation verändert sich das Symbol von Kaspersky Anti-Virus:

	Die Untersuchung einer E-Mail-Nachricht wird ausgeführt.
	Die Skriptuntersuchung wird ausgeführt.
	Die Untersuchung einer Datei, die von Ihnen oder einem Programm geöffnet, gespeichert oder gestartet wird, wird ausgeführt.
	Das Update der Datenbanken und Programm-Module von Kaspersky Anti-Virus wird ausgeführt.
	Der Neustart des Computers ist erforderlich, um Updates zu übernehmen.
	Bei der Arbeit einer Komponente von Kaspersky Anti-Virus ist eine Störung aufgetreten.

Das Symbol bietet außerdem Zugriff auf die grundlegenden Elemente der Programmoberfläche: Kontextmenü (s. Pkt. 4.2 auf S. 46) und Hauptfenster (s. Pkt. 4.3 auf S. 48).

Um das Kontextmenü zu öffnen, klicken Sie mit der rechten Maustaste auf das Programmsymbol.

Um das Hauptfenster von Kaspersky Anti-Virus im Abschnitt **Schutz** zu öffnen (mit diesem Abschnitt startet das Programm standardmäßig), doppelklicken Sie mit der linken Maustaste auf das Programmsymbol. Durch einfaches Klicken wird das Hauptfenster in dem Abschnitt geöffnet, der aktiv war, bevor es geschlossen wurde.

Wenn Nachrichten von Kaspersky Lab erscheinen, wird das Symbol im Infobereich der Taskleiste von Microsoft Windows eingeblendet. Durch Doppelklick mit der linken Maustaste wird ein Fenster mit dem Nachrichtentext geöffnet.

4.2. Kontextmenü

Das Kontextmenü (s. Abb. 1) bietet Zugriff auf die wichtigsten Schutzaufgaben.

Das Menü von Kaspersky Anti-Virus enthält folgende Punkte:

Arbeitsplatz untersuchen – Starten der vollständigen Untersuchung Ihres Computers auf das Vorhandensein von Viren. Dadurch werden die Objekte auf allen Laufwerken einschließlich der Wechseldatenträger untersucht.

Virensuche – Zur Auswahl von Objekten und zum Start der Virensuche in diesen Objekten wechseln. Standardmäßig enthält die Liste bestimmte Objekte wie beispielsweise den Ordner **Eigene Dateien**, Autostart-Objekte, Mailboxen, alle Laufwerke Ihres Computers usw. Sie können die Liste ergänzen, Objekte zur Untersuchung auswählen und die Virensuche starten.

Update – Starten der Aktualisierung der Datenbanken und Module von Kaspersky Anti-Virus und der Installation der Updates auf Ihrem Computer.

Abbildung 1. Kontextmenü

Aktivierung – Zum Aktivieren des Programms wechseln. Um den Status eines registrierten Benutzers zu erhalten, auf dessen Basis Ihnen die volle Funktionsfähigkeit der Anwendung und die Leistungen des Technischen Support-Services zur Verfügung gestellt werden, ist es erforderlich, Kaspersky Anti-Virus zu aktivieren. Dieser Menüpunkt ist nur vorhanden, wenn das Programm noch nicht aktiviert wurde.

Einstellungen – Zur Ansicht und Konfiguration der Funktionsparameter von Kaspersky Anti-Virus wechseln.

Kaspersky Anti-Virus – Das Programmhauptfenster öffnen (s. Pkt. 4.3 auf S. 48).

Schutz anhalten / Schutz aktivieren – Die Arbeit der Echtzeitschutz-Komponenten (s. Pkt. 2.2.1 auf S. 23) vorübergehend deaktivieren/aktivieren. Dieser Menüpunkt hat keinen Einfluss auf das Programm-Update und die Ausführung der Aufgaben zur Virenuntersuchung.

Über das Programm – Öffnen des Informationsfensters über Kaspersky Anti-Virus.

Beenden – Die Arbeit von Kaspersky Anti-Virus beenden (Bei Auswahl dieses Menüpunkts wird die Anwendung aus dem Arbeitsspeicher des Computers entfernt).

Wenn im Moment eine Aufgabe zur Virensuche läuft, wird ihr Name im Kontextmenü mit Prozentangabe des Ausführungsergebnisses angezeigt. Durch die Auswahl der Aufgabe gelangen Sie in das Berichtsfenster mit den aktuellen Ausführungsergebnissen.

4.3. Programmhauptfenster

Das Hauptfenster von Kaspersky Anti-Virus (s. Abb. 2) lässt sich in drei Bereiche aufteilen:

- Der obere Bereich des Fensters bietet einen Überblick über den aktuellen Schutzstatus Ihres Computers.

  Es existieren drei Möglichkeiten für den Zustand des Schutzes (s. Pkt. 5.1 auf S. 55). Jeder Zustand wird anschaulich durch eine bestimmte Farbe dargestellt. Die Farben entsprechen den Signalen einer Verkehrsampel. Grün bedeutet, dass der Schutz Ihres Computers dem erforderlichen Niveau entspricht. Gelb und Rot signalisieren, dass in den Einstellungen oder bei der Arbeit von Kaspersky Anti-Virus bestimmte Probleme vorhanden sind.

  Um ausführliche Informationen über diese Probleme zu erhalten und die Probleme schnell zu beheben, verwenden Sie den Sicherheitsassistenten. Der Assistent wird mit dem entsprechenden Link aus der Meldung über Sicherheitsrisiken geöffnet.

Abbildung 2. Hauptfenster von Kaspersky Anti-Virus

- Die linke Seite des Fensters, der *Navigationsbereich*, erlaubt es, schnell und einfach zu einer beliebigen Komponente, zur Ausführung der Aufgaben zur Virensuche, zum Update oder zu den Servicefunktionen des Programms zu wechseln.
- Die rechte Seite des Fensters, der *Informationsbereich*, enthält Informationen über die auf der linken Seite ausgewählte Schutzkomponente, erlaubt den Wechsel zu den Einstellungen der einzelnen Komponenten, bietet Werkzeuge zur Ausführung der Aufgaben zur Virensuche, zur Arbeit mit Dateien in der Quarantäne und im Backup, zur Verwaltung der Lizenzschlüssel usw.

Wird auf der linken Fensterseite ein Abschnitt oder eine Komponente ausgewählt, dann erhalten Sie auf der rechten Seite vollständige Informationen darüber.

Hier werden die Elemente der Navigationsleiste des Hauptfensters genauer beschrieben.

Abschnitt des Navigationsteils im Hauptfenster	Funktion
	Die Hauptaufgabe des Abschnitts **Schutz** besteht darin, den Zugriff auf die Hauptkomponenten des Echtzeitschutzes für Ihren Computer zu gewährleisten. Um ausführliche Informationen über die Arbeit einer Schutzkomponente oder deren Module zu erhalten, wechseln Sie zu den Einstellungen der Komponente oder wählen Sie die Komponente in der Liste des Abschnitts **Schutz** aus und öffnen Sie den Bericht. Außerdem befinden sich in diesem Abschnitt Links, die dem Zugriff auf häufig benötigte Aufgaben dienen: Virenuntersuchung bestimmter Objekte und Update der Programm-Datenbanken. Sie können Informationen über den Status dieser Aufgaben anzeigen, die Aufgaben anpassen oder sie sofort starten.

Abschnitt des Navigationsteils im Hauptfenster	**Funktion**
	Der Abschnitt **Virensuche** gewährleistet den Zugriff auf Aufgaben zur Virenuntersuchung von Objekten. Er enthält Aufgaben, die von den Kaspersky-Lab-Experten erstellt wurden (Virensuche in kritischen Bereichen, Virensuche in Autostart-Objekten, vollständige Untersuchung des Computers, Suche nach Rootkits), sowie die vom Benutzer erstellten Aufgaben. Wenn Sie in der Liste auf der rechten Seite des Fensters eine Aufgabe wählen, können Sie Informationen über die Ausführung der Aufgabe ansehen, zu den Einstellungen der Aufgabe wechseln, die Liste der Untersuchungsobjekte bearbeiten oder die Ausführung der Aufgabe starten. Wählen Sie zur Untersuchung eines einzelnen Objekts (Datei, Ordner oder Laufwerk) den Abschnitt **Virensuche**, fügen Sie das Objekt zur Liste der Untersuchungsobjekte hinzu und starten Sie die Aufgabe. Außerdem bietet dieser Abschnitt Zugriff auf die Funktion zum Erstellen einer fall-CD zur Systemwiederherstellung (s. 15.4 auf S. 204).

Abschnitt des Navigationsteils im Hauptfenster	Funktion
	Der Abschnitt **Update** enthält Informationen über die Aktualisierung der Anwendung: Erscheinungsdatum der Datenbanken und Anzahl der in den Datenbanken enthaltenen Virensignaturen. Mit Hilfe der entsprechenden Links können Sie die Aktualisierung starten, einen ausführlichen Bericht ansehen, zu den Update-Einstellungen wechseln oder das Update rückgängig machen.
	Im Abschnitt **Datenverwaltung** können Sie einen ausführlichen Bericht über die Arbeit einer beliebigen Anwendungskomponente, Untersuchung- oder Update-Aufgabe (s. Pkt. 15.3 auf S. 195) anzeigen und zur Arbeit mit Objekten, die sich in der Quarantäne (s. Pkt. 15.1 auf S. 188) oder im Backup (s. Pkt. 15.2 auf S. 193) befinden, wechseln.
	Der Abschnitt **Aktivierung** dient der Verwaltung von Schlüsseln, die für die vollfunktionale Arbeit der Anwendung erforderlich sind (s. Kapitel 14 auf S. 185). Wenn kein Schlüssel installiert ist, wird empfohlen, möglichst schnell einen Schlüssel zu kaufen und die Anwendung zu aktivieren (s. Pkt. 3.2.2 auf S. 36). Ist ein Schlüssel installiert, dann enthält dieser Abschnitt Informationen über den Typ und die Gültigkeitsdauer des verwendeten Schlüssels. Bei Ablauf der Gültigkeitsdauer des aktiven Schlüssels können Sie diesen über die Kaspersky-Lab-Webseite verlängern.

Abschnitt des Navigationsteils im Hauptfenster	Funktion
	Im Abschnitt **Support** befinden sich Informationen über die Angebote des Technischen Support-Services für die registrierten Benutzer von Kaspersky Anti-Virus.

Jedes Element des Navigationsbereichs verfügt über ein spezielles Kontextmenü. Für die Schutzkomponenten enthält das Menü beispielsweise Punkte, die es erlauben, schnell zu deren Einstellungen, zur Steuerung oder zur Berichtsansicht zu gelangen. Für die Aufgaben zur Virensuche ist ein zusätzlicher Menüpunkt vorgesehen, der es erlaubt, auf Basis der ausgewählten Aufgabe eine neue Aufgabe zu erstellen.

Sie können das Aussehen des Programms anpassen, indem Sie grafische Elemente und Farbschemen erstellen und verwenden.

Auf der linken Seite des Fensters befinden sich die beiden Schaltflächen **Hilfe**, für den Zugriff auf das Hilfesystem von Kaspersky Anti-Virus, und **Einstellungen**, mit der das Konfigurationsfenster des Programms geöffnet werden kann.

4.4. Konfigurationsfenster des Programms

Das Konfigurationsfenster von Kaspersky Anti-Virus kann aus dem Hauptfenster (s. Pkt. 4.3 auf S. 48) oder aus dem Kontextmenü (s. Pkt. 4.2 auf S. 46) der Anwendung geöffnet werden. Klicken Sie dazu auf den Link **Einstellungen** im unteren Bereich des Hauptfensters oder wählen Sie den gleichnamigen Punkt im Kontextmenü der Anwendung.

Die Struktur des Konfigurationsfensters (s. Abb. 3) entspricht jener des Hauptfensters:

- Die linke Seite des Fensters bietet schnellen und bequemen Zugriff auf Einstellungen für jede Echtzeitschutz-Komponente, für die Untersuchungsaufgaben und für das Update sowie auf die Einstellungen für die Servicefunktionen der Anwendung.
- Die rechte Seite des Fensters enthält eine Liste der Parameter für die auf der linken Seite ausgewählte Komponente, Aufgabe usw.

Wird auf der linken Seite des Konfigurationsfensters ein bestimmter Abschnitt, eine Komponente oder eine Aufgabe ausgewählt, dann werden auf der rechten

Fensterseite die entsprechenden Parameter angezeigt. Zur Detaileinstellung bestimmter Parameter können Sie die Konfigurationsfenster der zweiten oder dritten Ebene öffnen. Eine ausführliche Beschreibung der Anwendungsparameter finden Sie in den Abschnitten des vorliegenden Benutzerhandbuchs.

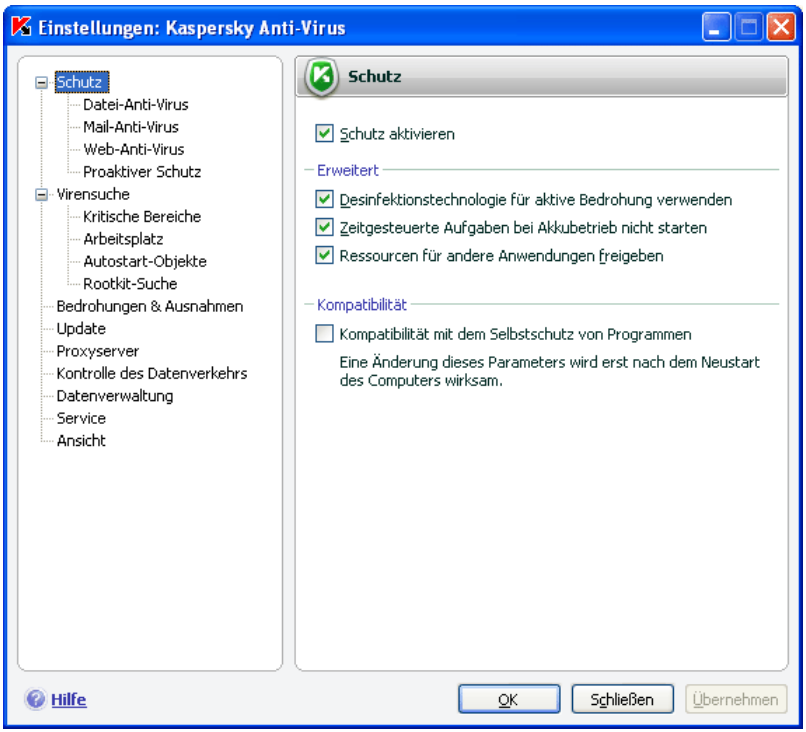


Abbildung 3. Konfigurationsfenster von Kaspersky Anti-Virus

KAPITEL 5. ERSTE SCHRITTE

Bei der Entwicklung von Kaspersky Anti-Virus bestand eine der Hauptaufgaben der Spezialisten von Kaspersky Lab in der optimalen Konfiguration aller Programmeinstellungen. Das verleiht einem Benutzer unabhängig von seiner Erfahrung mit Computern die Möglichkeit, sofort nach der Programminstallation die Sicherheit des Computers zu gewährleisten, ohne sich ausführlich mit den Einstellungen zu beschäftigen.

Allerdings können die Konfiguration Ihres Computers oder die auf diesem zu lösenden Aufgaben Besonderheiten aufweisen. Deshalb empfehlen wir Ihnen, das Programm zuerst anzupassen, um mit den Schutz mit maximaler Flexibilität genau auf Ihren Computer einzustellen.

Um die Benutzerfreundlichkeit zu erhöhen, haben wir uns bemüht, die Etappen der vorbereitenden Einstellungen in dem Konfigurationsassistenten (s. Pkt. 3.2 auf S. 35) zusammenzufassen, der am Ende der Programminstallation gestartet wird. Im Rahmen des Assistenten können Sie das Programm aktivieren, Einstellungen für das Update und den Start von Untersuchungsaufgaben vornehmen und den Zugriff auf das Programm mit Hilfe eines Kennworts beschränken.

Wir empfehlen Ihnen, nach der Installation und dem Start des Programms auf Ihrem Computer folgende Aktionen vorzunehmen:

- Bewertung des aktuellen Schutzstatus, um sicherzustellen, dass Kaspersky Anti-Virus den Schutz auf der erforderlichen Stufe gewährleistet (s. Pkt. 5.1 auf S. 55).
- Update des Programms, wenn das Update nicht mit Hilfe des Konfigurationsassistenten oder automatisch sofort nach der Programminstallation erfolgte (s. Pkt. 5.6 auf S. 61).
- Untersuchung des Computers auf das Vorhandensein von Viren (s. Pkt. 5.3 auf S. 59).

5.1. Welchen Schutzstatus hat der Computer?

Der Schutzstatus Ihres Computers informiert darüber, ob im Augenblick Bedrohungen vorhanden sind, die das Gesamtniveau der Systemsicherheit beeinflussen. Als Bedrohungen gelten in diesem Fall nicht nur der Fund schädlicher Programme, sondern auch die Verwendung veralteter Datenbanken, die Inaktivität

bestimmter Schutzkomponenten, die Auswahl einer niedrigen Sicherheitsstufe u.a.

Der Schutzstatus wird im oberen Bereich des Programmhauptfensters angezeigt und durch Farben dargestellt, die denen einer Verkehrsampel entsprechen. Abhängig von der Situation ändern sich die im oberen Fensterbereich angezeigten Farben. Wenn im Sicherheitssystem Bedrohungen vorhanden sind, werden zusätzlich Textinformationen angezeigt, die die Form eines Links zum Sicherheitsassistenten besitzen.

Der Schutzstatus kann durch eine der folgenden Farben signalisiert werden:

- Grundfarbe des Hauptfensters - *grün*. Dieser Status weist darauf hin, dass der Schutz Ihres Computers dem erforderlichen Niveau entspricht.

  Das bedeutet, dass die Datenbanken der Anwendung rechtzeitig aktualisiert wurden, dass alle Anwendungskomponenten aktiviert sind, dass die Anwendung mit Parametern arbeitet, die von den Kaspersky-Lab-Spezialisten empfohlen werden, und dass bei der vollständigen Untersuchung des Computers keine schädlichen Objekte gefunden oder gefundene schädliche Objekte neutralisiert wurden.

- Grundfarbe des Hauptfensters - *gelb*. Der Schutzstatus Ihres Computers liegt unter dem Niveau des zuvor beschriebenen Status. Dieser Schutzstatus weist darauf hin, dass bei der Arbeit oder in den Einstellungen der Anwendung bestimmte Probleme vorliegen.

  Dieser Status tritt beispielsweise ein, wenn geringfügige Abweichungen vom empfohlenen Funktionsmodus bestehen, die Datenbanken seit mehreren Tagen nicht mehr aktualisiert wurden oder das Anti-Spam-Training noch nicht erfolgt ist.

- Grundfarbe des Hauptfensters - *rot.* Ihr Computer unterliegt einer ernsthaften Infektionsgefahr. Dieser Status signalisiert die Existenz von Problemen, die zur Infektion des Computers und zu Datenverlust führen können.

  Das ist beispielsweise der Fall, wenn es bei der Arbeit einer oder mehrerer Schutzkomponenten zu Störungen gekommen ist, die Anwendung sehr lange nicht mehr aktualisiert wurde, schädliche Objekte gefunden wurden, die dringend neutralisiert werden müssen, oder die Anwendung noch nicht aktiviert wurde.

Im Schutzsystem vorhandene Probleme sollten umgehend behoben werden. Verwenden Sie dazu den Sicherheitsassistenten, der mit Hilfe des Links in der Meldung über im Sicherheitssystem vorhandene Bedrohungen geöffnet wird. Der Sicherheitsassistent unterstützt Sie dabei, vorhandene Bedrohungen zu prüfen und sofort zu beseitigen. Die Priorität einer Bedrohung wird durch die Farbe des Indikators dargestellt:

– *Der Indikator weist darauf hin, dass unkritische Bedrohungen vorliegen*, die aber zu einer verminderten Schutzstufe des Computers führen können. Bitte beachten Sie die Empfehlungen der Kaspersky-Lab-Spezialisten.

– *Der Indikator weist auf das Vorhandensein ernsthafter Bedrohungen* für den Schutz Ihres Computers hin. Bitte folgen Sie genau den darunter angegebenen Empfehlungen. Alle Anweisungen dienen dazu, den Schutz Ihres Computers zu optimieren. Die empfohlenen Aktionen besitzen die Form von Links.

Um eine Liste der vorhandenen Bedrohungen anzuzeigen, verwenden Sie den Link Weiter. Für jede Bedrohung sind eine ausführliche Beschreibung und eine Auswahl von Aktionen vorhanden:

- *Bedrohung sofort neutralisieren*. Mit Hilfe der entsprechenden Links können Sie zur sofortigen Neutralisierung der Bedrohung übergehen. Um ausführliche Informationen über Ereignisse, die mit dem Auftreten dieser Bedrohung verbunden sind, zu erhalten, können Sie die Berichtsdatei konsultieren. Die sofortige Neutralisierung einer Bedrohung entspricht der empfohlenen Aktion.

- *Neutralisierung der Bedrohung aufschieben*. Wenn Sie eine Bedrohung aufgrund bestimmter Umstände nicht sofort beseitigen können, kann diese Aktion aufgeschoben werden und Sie können später dazu zurückkehren. Verwenden Sie dazu den Link Aufschieben.

  Beachten Sie, dass diese Möglichkeit für kritische Bedrohungen nicht vorgesehen ist. Dazu gehören beispielsweise die Existenz von nicht neutralisierten Schädlingen, Störungen bei der Arbeit einer oder mehrerer Komponenten und beschädigte Dateien der Programm-Datenbanken.

Wenn beim Abschluss des Sicherheitsassistenten noch nicht neutralisierte Bedrohungen vorhanden sind, erscheint im oberen Bereich des Anwendungshauptfensters ein Hinweis, der an die notwendige Neutralisierung erinnert. Wird der Sicherheitsassistent wiederholt geöffnet, dann werden zurückgestellte Bedrohungen nicht in der Liste der aktiven Bedrohungen angezeigt. Zur Liste der aufgeschobenen Bedrohungen und zu deren Neutralisierung können Sie im letzten Fenster des Assistenten durch Klick auf den Link Bedrohungen anzeigen, deren Lösung aufgeschoben wurde zurückkehren.

5.2. Status einer bestimmten Schutzkomponente

Um den Status einer beliebigen Komponente des Echtzeitschutzes anzuzeigen, öffnen Sie das Programmhauptfenster und wählen Sie im Abschnitt **Schutz** die Komponente aus. Dadurch werden auf der rechten Seite des Fensters zusammenfassende Informationen über die Arbeit der gewählten Komponente angezeigt.

Die wichtigste Information ist der Funktionsstatus der Komponente:

- <*Komponente*> : aktiv – Der Schutz, der durch diese Komponente gewährleistet wird, funktioniert auf der erforderlichen Stufe.
- <*Komponente*> *: Pause* – Die Komponente wurde für einen bestimmten Zeitraum angehalten. Der Schutz wird nach Ablauf des festgelegten Zeitraums oder nach dem Neustart des Programms automatisch fortgesetzt. Sie können die Komponente manuell aktivieren. Verwenden Sie dazu den Link Arbeit fortsetzen.
- <*Komponente*> *: deaktiviert* – Die Arbeit der Komponente wurde vom Benutzer beendet. Sie können den Schutz aktivieren. Verwenden Sie dazu den Link Aktivieren.
- <*Komponente*> *: funktioniert nicht* – Der Schutz, der durch diese Komponente gewährleistet wird, ist aus bestimmten Gründen nicht verfügbar.
- <*Komponente*> *: Störung*– Die Komponente hat ihre Arbeit fehlerhaft abgeschlossen.

  Wenn bei der Arbeit der Komponente ein Fehler auftritt, versuchen Sie sie erneut zu starten. Sollte auch der wiederholte Start fehlerhaft verlaufen, dann prüfen Sie den Bericht über die Arbeit der Komponente. Möglicherweise finden Sie dort den Grund der Störung. Wenn Sie das Problem nicht selbst lösen können, speichern Sie den Bericht über die Arbeit der Komponente mit der Schaltfläche **Aktionen → Speichern unter** in einer Datei und wenden Sie sich an den Technischen Support-Service von Kaspersky Lab.

Unter dem Funktionsstatus der Komponente werden Informationen über die Einstellungen, mit denen die Komponente arbeitet genannt (z.B. Sicherheitsstufe; Aktion, die auf gefährliche Objekte angewandt wird). Wenn die Komponente aus mehreren Modulen besteht, wird deren Status angegeben, d.h. ob sie aktiv oder deaktiviert sind. Verwenden Sie den Link Anpassen, um die aktuellen Einstellungen für die Arbeit der Komponente zu ändern.

Außerdem können statistische Angaben über die Arbeitsergebnisse jeder Komponente angezeigt werden. Verwenden Sie den Link Bericht öffnen, um den Bericht anzuschauen.

Wenn die Komponente im Augenblick deaktiviert oder angehalten ist, können Sie die bisherigen Arbeitsergebnisse anzeigen. Verwenden Sie dazu den Link Bericht über den letzten Start öffnen.

5.3. Wie der Computer auf Viren untersucht wird

Nach der Installation der Anwendung werden Sie durch eine obligatorische Meldung im unteren linken Bereich des Programmfensters darauf hingewiesen, dass noch keine Untersuchung des Computers ausgeführt wurde, und Ihnen wird empfohlen, ihn umgehend auf Viren zu untersuchen.

Der Lieferumfang von Kaspersky Anti-Virus umfasst eine Aufgabe zur Virensuche auf dem Computer. Diese befindet sich im Abschnitt **Virensuche** des Programmhauptfensters.

Nach der Auswahl der Aufgabe **Arbeitsplatz** können Sie die Aufgabenparameter überprüfen (welche Sicherheitsstufe wurde gewählt, welche Aktion wird auf gefährliche Objekte angewandt) und den Bericht über den letzten Start der Aufgabe ansehen.

Um den Computer auf die Existenz von schädlichen Objekten zu untersuchen,

1. Wählen Sie im Programmhauptfenster im Abschnitt **Virensuche** die Aufgabe **Arbeitsplatz**.
2. Klicken Sie auf den Link Untersuchung starten.

Dadurch wird die Untersuchung Ihres Computers gestartet. Details der Untersuchung werden in einem speziellen Fenster angezeigt. Durch Klick auf die Schaltfläche **Schließen** wird das Fenster mit Informationen über den Untersuchungsvorgang ausgeblendet. Die Untersuchung wird dadurch nicht beendet.

5.4. Wie kritische Computerbereiche untersucht werden

Auf Ihrem Computer gibt es Bereiche, die hinsichtlich der Sicherheit als kritisch gelten. Sie können zum Objekt einer Infektion durch schädliche Programme wer-

den, die auf die Beschädigung des Computerbetriebssystems, Prozessors, Arbeitsspeichers usw. gerichtet ist.

Es ist äußerst wichtig, die kritischen Bereiche des Computers zu schützen, um seine Funktionsfähigkeit aufrechtzuerhalten. Kaspersky Anti-Virus bietet eine spezielle Aufgabe zur Virensuche in diesen Bereichen. Sie befindet sich im Abschnitt **Virensuche** des Programmhauptfensters.

Nach der Auswahl der Aufgabe **Kritische Bereiche** können Sie die Aufgabenparameter überprüfen (welche Sicherheitsstufe wurde gewählt, welche Aktion wird auf gefährliche Objekte angewandt). Hier kann auch festgelegt werden, welche kritischen Bereiche untersucht werden sollen. Außerdem kann hier die Virensuche in den ausgewählten Bereichen gestartet werden.

Um die kritischen Computerbereiche auf die Existenz von schädlichen Objekten zu untersuchen,

1. Wählen Sie im Programmhauptfenster im Abschnitt **Virensuche** die Aufgabe **Kritische Bereiche**.
2. Klicken Sie auf den Link Untersuchung starten.

Dadurch wird die Untersuchung der ausgewählten Bereiche gestartet. Details der Untersuchung werden in einem speziellen Fenster angezeigt. Durch Klick auf die Schaltfläche **Schließen** wird das Fenster mit Informationen über den Untersuchungsvorgang ausgeblendet. Die Untersuchung wird dadurch nicht beendet.

5.5. Wie eine Datei, ein Ordner oder ein Laufwerk auf Viren untersucht werden

In bestimmten Situationen ist es erforderlich, nicht den gesamten Computer zu untersuchen, sondern nur ein einzelnes Objekt wie beispielsweise eine Festplatte, auf der sich Programme und Spiele befinden, Mail-Datenbanken, die aus dem Büro mitgebracht wurden, ein Archiv, das per E-Mail empfangen wurde, usw. Sie können ein Objekt mit den Standardmitteln von Microsoft Windows auswählen (beispielsweise im Fenster des Programms **Explorer** oder auf dem **Arbeitsplatz** usw.).

Um die Untersuchung des Objekts zu starten,

führen Sie den Mauscursor auf den Namen des gewählten Objekts, öffnen durch Rechtsklick das Microsoft Windows-Kontextmenü und wählen den Punkt **Auf Viren untersuchen** (s. Abb. 4).

Dadurch wird die Untersuchung des ausgewählten Objekts gestartet. Details der Untersuchung werden in einem speziellen Fenster angezeigt. Durch Klick auf die Schaltfläche **Schließen** wird das Fenster mit Informationen über den Untersuchungsvorgang ausgeblendet. Die Untersuchung wird dadurch nicht beendet.

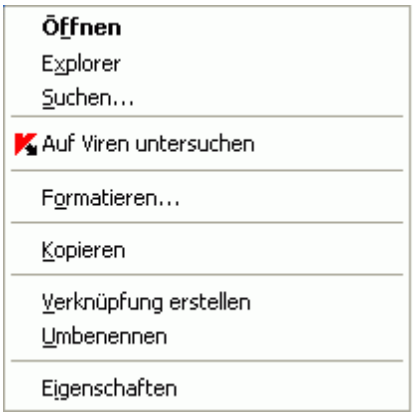


Abbildung 4. Virenuntersuchung eines Objekts, das über Microsoft Windows ausgewählt wurde

5.6. Wie das Programm aktualisiert wird

Kaspersky Lab aktualisiert die Datenbanken und die internen Module von Kaspersky Anti-Virus und verwendet dazu spezielle Updateserver.

Kaspersky-Lab-Updateserver sind Internetseiten von Kaspersky Lab, auf denen Programm-Updates zur Verfügung stehen.

Achtung!

Für das Update von Kaspersky Anti-Virus ist eine bestehende Internetverbindung erforderlich.

Kaspersky Anti-Virus überprüft in der Grundeinstellung automatisch, ob auf den Kaspersky-Lab-Servern neue Updates vorhanden sind. Wenn auf dem Server neue Updates angeboten werden, lädt Kaspersky Anti-Virus sie im Hintergrundmodus herunter und installiert sie.

Um Kaspersky Anti-Virus manuell zu aktualisieren,

1. Wählen Sie im Programmhauptfenster den Abschnitt **Update**.

2. Klicken Sie auf den Link Datenbanken aktualisieren.

Dadurch wird die Aktualisierung von Kaspersky Anti-Virus gestartet. Alle Details über den Prozess werden in einem speziellen Fenster angezeigt.

5.7. Was tun, wenn der Schutz nicht funktioniert?

Sollten bei der Arbeit einer beliebigen Schutzkomponente Probleme oder Fehler auftreten, beachten Sie unbedingt ihren Status. Wenn als Status der Komponente *funktioniert nicht* oder *Störung* angezeigt wird, versuchen Sie, Kaspersky Anti-Virus neu zu starten.

Sollte das Problem nach dem Neustart der Anwendung weiter bestehen, wird empfohlen, mögliche Fehler mit Hilfe des Reparaturprogramms für die Anwendung zu korrigieren (s. Kapitel 17 auf S. 250).

Falls der Reparaturversuch erfolglos sein sollte, wenden Sie sich an den technischen Support-Service von Kaspersky Lab. Es kann erforderlich sein, den Bericht über die Arbeit der Komponente in einer Datei zu speichern und ihn zur Analyse an den Support-Service zu schicken.

Um den Bericht über die Arbeit einer einzelnen Komponente in einer Datei zu speichern,

1. Wählen Sie die Komponente im Abschnitt **Schutz** des Programmhauptfensters und verwenden Sie den Link Bericht öffnen (wenn die Komponente momentan aktiv ist) oder den Link Bericht über den letzten Start öffnen (wenn die Komponente deaktiviert ist).
2. Klicken Sie im Berichtsfenster auf die Schaltfläche **Aktionen → Speichern unter** und geben Sie im folgenden Fenster den Namen der Datei an, in welcher die Arbeitsergebnisse der Komponente gespeichert werden sollen.

KAPITEL 6. KOMPLEXE STEUERUNG DES SCHUTZES

Dieser Abschnitt enthält Informationen über die Konfiguration der allgemeinen Anwendungsparameter, die bei der Arbeit aller Echtzeitschutz-Komponenten und Aufgaben verwendet werden. Außerdem werden hier die Definition des Schutzbereichs bzw. einer Liste der Bedrohungen, vor denen die Anwendung schützt, und eine Liste der vertrauenswürdigen Objekte, die vom Schutz ausgeschlossen werden sollen, behandelt.

- Steuerung des Echtzeitschutzes des Computers (s. Pkt. 6.1 auf S. 63).
- Verwendung der Technologie zur Desinfektion einer aktiven Bedrohung (s. Pkt. 6.2 auf S. 67).
- Start von Aufgaben bei der Arbeit auf einem Laptop (s. Pkt. 6.3 auf S. 68).
- Gleichzeitige Arbeit von Kaspersky Anti-Virus und anderen Programmen (s. Pkt. 6.4 auf S. 68).
- Kompatibilität von Kaspersky Anti-Virus mit dem Selbstschutz anderer Programme (s. Pkt. 6.5 auf S. 69).
- Liste der Bedrohungen (s. Pkt. 6.8 auf S. 73), vor denen die Anwendung schützen soll.
- Liste von Objekten der vertrauenswürdigen Zone (s. Pkt. 6.9 auf S. 75), die vom Schutz ausgeschlossen werden sollen.

6.1. Echtzeitschutz des Computers deaktivieren/aktivieren

Kaspersky Anti-Virus wird standardmäßig beim Start des Betriebssystems gestartet, worüber Sie durch den Hinweis *Kaspersky Anti-Virus 7.0* rechts oben auf dem Bildschirm informiert werden, und schützt Ihren Computer während der gesamten Sitzung. Alle Echtzeitschutz-Komponenten sind aktiv (s. Pkt. 2.2.1 auf S. 23).

Sie können den von Kaspersky Anti-Virus gewährleisteten Schutz vollständig oder teilweise deaktivieren.

Achtung!

Sie Kaspersky-Lab-Spezialisten **warnen ausdrücklich davor, den Echtzeitschutz zu deaktivieren**, weil dies zur Infektion Ihres Computers und zu Datenverlust führen kann.

Beachten Sie, dass der Schutz hier ausdrücklich im Kontext der Schutzkomponenten beschrieben wird. Das Deaktivieren oder das Anhalten der Arbeit von Schutzkomponenten übt keinen Einfluss auf die Ausführung von Aufgaben zur Virensuche und auf das Programm-Update aus.

6.1.1. Schutz anhalten

Das Anhalten des Echtzeitschutzes bedeutet, dass alle seine Komponenten, welche die Dateien auf Ihrem Computer, eingehende und ausgehende Post, auszuführende Skripts und das Verhalten der Anwendungen kontrollieren, für einen bestimmten Zeitraum deaktiviert werden.

Um den Echtzeitschutz des Computers anzuhalten,

1. Wählen Sie im Kontextmenü (s. Pkt. 4.2 auf S. 46) des Programms den Punkt **Schutz anhalten**.
2. Wählen Sie im folgenden Fenster zum Deaktivieren des Schutzes (s. Abb. 5) den Zeitraum, nach dem der Schutz wieder aktiviert werden soll:
   - In <Zeitraum> – Der Schutz wird nach Ablauf des festgelegten Zeitraums wieder aktiviert. Verwenden Sie die Dropdown-Liste, um den Wert für das Zeitintervall festzulegen.
   - Nach dem Neustart des Programms – Der Schutz wird aktiviert, wenn Sie das Programm aus dem Menü **Start** starten oder nachdem das System neu gestartet wurde (unter der Bedingung, dass der Modus für den Programmstart beim Hochfahren des Computers aktiviert ist (s. Pkt. 15.11 auf S. 231).
   - Nur auf Befehl des Benutzers – Der Schutz wird erst dann wieder aktiviert, wenn Sie ihn starten. Wählen Sie den Punkt **Schutz aktivieren** im Kontextmenü des Programms, um den Schutz zu aktivieren.

Durch das vorübergehende Deaktivieren wird die Arbeit aller Schutzkomponenten angehalten. Darüber informieren:

- Die inaktiven (graue Farbe) Namen der deaktivierten Komponenten im Abschnitt **Schutz** des Hauptfensters.
- Das inaktive (graue) Programmsymbol im Infobereich der Taskleiste von Microsoft Windows.

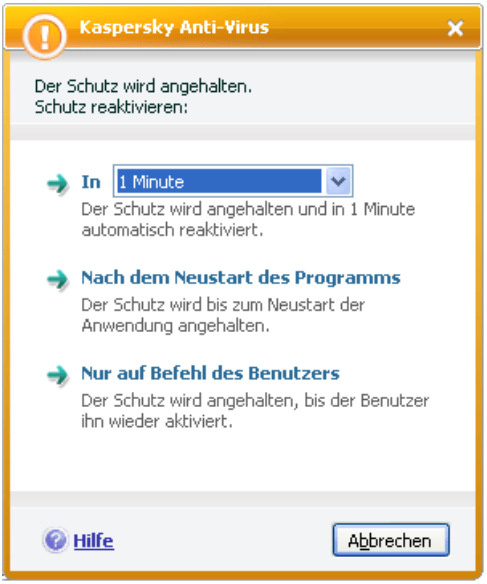

Kaspersky Anti-Virus
Der Schutz wird angehalten.
Schutz reaktivieren:
In
1 Minute
Der Schutz wird angehalten und in 1 Minute automatisch reaktiviert.
Nach dem Neustart des Programms
Der Schutz wird bis zum Neustart der Anwendung angehalten.
Nur auf Befehl des Benutzers
Der Schutz wird angehalten, bis der Benutzer ihn wieder aktiviert.
Hilfe
Abbrechen

Abbildung 5. Fenster zum Anhalten des Computerschutzes

6.1.2. Computerschutz vollständig deaktivieren

Das vollständige Deaktivieren des Schutzes bedeutet, dass die Arbeit der Echtzeitschutz-Komponenten beendet wird. Die Virensuche und das Update funktionieren weiterhin im vorgegebenen Modus.

Wenn der Schutz vollständig deaktiviert wurde, kann er nur auf Befehl des Benutzers wieder aktiviert werden. In diesem Fall erfolgt kein automatisches Aktivieren der Schutzkomponenten nach dem Neustart des Systems oder des Programms. Beachten Sie, dass bei Konflikten zwischen Kaspersky Anti-Virus und anderen auf Ihrem Computer installierten Programmen die Arbeit einer einzelnen Schutzkomponente angehalten oder eine Liste von Ausnahmen angelegt werden kann (s. Pkt. 6.9 auf S. 75).

Um den Echtzeitschutz des Computers vollständig zu deaktivieren,

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie den Abschnitt **Schutz**.
2. Deaktivieren Sie das Kontrollkästchen **Schutz aktivieren**.

Durch das Deaktivieren des Schutzes wird die Arbeit aller seiner Komponenten beendet. Darüber informieren:

- Die inaktiven (grauen) Namen der deaktivierten Komponenten im Abschnitt **Schutz** des Hauptfensters.
- Das inaktive (graue) Programmsymbol im Infobereich der Taskleiste von Microsoft Windows.

6.1.3. Einzelne Schutzkomponenten anhalten/beenden

Es gibt mehrere Methoden, um die Arbeit einer Schutzkomponente zu deaktivieren. Bevor eine Komponente deaktiviert wird, Sie allerdings Ihre Gründe dafür genau abwägen. Höchstwahrscheinlich besteht eine andere Möglichkeit, beispielsweise die Wahl einer anderen Sicherheitsstufe. Wenn Sie beispielsweise mit einer bestimmten Datenbank arbeiten, von der Sie sicher sind, dass sie virenfrei ist, geben Sie das Verzeichnis mit ihren Dateien einfach als Ausnahme an (s. Pkt. 6.9 auf S. 75).

Um eine einzelne Schutzkomponente anzuhalten,

öffnen Sie das Programmhauptfenster, wählen Sie im Abschnitt **Schutz** die Komponente und verwenden Sie den Link Pause.

Der Status der Komponente ändert sich in *Pause*. Der durch die Komponente gewährleistete Schutz wird angehalten, bis Sie die Anwendung neu starten oder die Komponente durch Klick auf den Link Arbeit fortsetzen wieder einschalten.

Wenn Sie eine Komponente anhalten, wird die Statistik in der laufenden Sitzung von Kaspersky Anti-Virus gespeichert. Die Statistik wird fortgeführt, wenn die Arbeit der Komponente wieder aufgenommen wird.

Um eine einzelne Schutzkomponente zu beenden,

öffnen Sie das Programmhauptfenster, wählen Sie im Abschnitt **Schutz** die Komponente und verwenden Sie den Link Stopp.

In diesem Fall ändert sich der Status der Komponente in *deaktiviert* (*abgebrochen*) und in der Komponentenliste des Abschnitts **Schutz** wird ihr Name

als inaktiv (graue Farbe) angezeigt. Der durch die Komponente gewährleistete Schutz wird beendet, bis Sie auf die Schaltfläche Aktivieren klicken.

Jede Komponente des Echtzeitschutzes kann auch aus dem Konfigurationsfenster des Programms beendet werden. Wählen Sie die Komponente dazu im Abschnitt **Schutz** aus und deaktivieren Sie das Kontrollkästchen **<Komponente> aktivieren**.

Beim Beenden einer Schutzkomponente wird die gesamte Statistik über die bisherige Arbeit zurückgesetzt und beim Start der Komponente neu erstellt.

Die Arbeit der einzelnen Schutzkomponenten wird auch beendet, wenn der Echtzeitschutz Ihres Computers vollständig deaktiviert wird (s. Pkt. 6.1.2 auf S. 65).

6.1.4. Computerschutz wiederherstellen

Wenn Sie zu einem gewissen Zeitpunkt den Echtzeitschutz Ihres Computers angehalten oder vollständig deaktiviert haben, dann kann er durch eine der folgenden Methoden wieder aktiviert werden:

- *Aus dem Kontextmenü*.

  Wählen Sie dazu den Punkt **Schutz aktivieren**.

- *Aus dem Programmhauptfenster*.

  Wählen Sie auf der linken Seite des Hauptfensters den Abschnitt **Schutz** und verwenden Sie im Kontextmenü den Link Start.

Der Schutzstatus ändert sich sofort in *aktiv*. Das Programmsymbol im Infobereich der Taskleiste von Microsoft Windows wird aktiv (farbig).

6.2. Technologie zur Desinfektion einer aktiven Infektion

Moderne Schadprogramme können auf die tiefsten Ebenen des Betriebssystems vordringen, wodurch es praktisch unmöglich wird, sie zu löschen. Wenn Kaspersky Anti-Virus eine Bedrohung erkennt, die momentan im System aktiv ist, bietet er an, einen speziell dafür vorgesehenen erweiterten Desinfektionsvorgang auszuführen, durch den die Bedrohung neutralisiert und vom Computer gelöscht wird.

Beim Abschluss des Vorgangs erfolgt der obligatorische Neustart des Computers. Nach dem Neustart des Computers wird empfohlen, die vollständige Virenuntersuchung zu starten. Damit der Vorgang zur erweiterten Desinfektion

verwendet wird, öffnen Sie das Konfigurationsfenster des Programms, wählen Sie den Abschnitt **Schutz** und aktivieren Sie im Block **Erweitert** (s. Abb. 6) das Kontrollkästchen ☑ **Desinfektionstechnologie für aktive Bedrohung verwenden**.

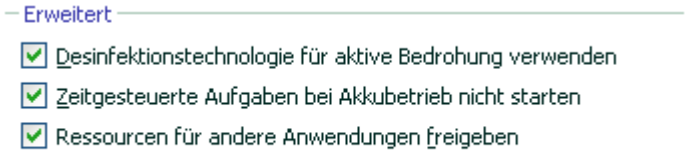

Erweitert
Desinfektionstechnologie für aktive Bedrohung verwenden
Zeitgesteuerte Aufgaben bei Akkubetrieb nicht starten
Ressourcen für andere Anwendungen freigeben

Abbildung 6. Anpassen allgemeiner Parameter

6.3. Arbeit der Anwendung auf einem Laptop

Um sparsam mit der Batterie eines Laptops umzugehen, können Sie festlegen, dass Aufgaben zur Virensuche aufgeschoben werden.

Da die Virensuche auf dem Computer und die Programmaktualisierung relativ viel Ressourcen und Zeit benötigen, empfehlen wir Ihnen, den zeitgesteuerten Start solcher Aufgaben zu deaktivieren. Dadurch können Sie Akkustrom sparen. Bei Bedarf können Sie das Programm selbständig aktualisieren (s. Pkt. 5.6 auf S. 61) oder die Virenuntersuchung starten (s. Pkt. 5.3 auf S. 59). Um den Dienst zum Stromsparen im Batteriebetrieb zu verwenden, öffnen Sie das Konfigurationsfenster des Programms, wählen Sie den Abschnitt **Schutz** und aktivieren Sie im Block **Erweitert** (s. Abb. 6) das Kontrollkästchen ☑ **Zeitgesteuerte Aufgaben bei Akkubetrieb nicht starten**.

6.4. Leistung des Computers beim Ausführen von Aufgaben

Um die Belastung des Prozessors und der Laufwerkssubsysteme zu beschränken, können Sie festlegen, dass Aufgaben zur Virensuche aufgeschoben werden.

Das Ausführen von Untersuchungsaufgaben erhöht die Belastung des Prozessors und der Laufwerkssubsysteme und verlangsamt dadurch die Arbeit anderer Programme. In der Grundeinstellung hält das Programm beim Eintreten

dieser Situation die Ausführung von Untersuchungsaufgaben an und gibt Systemressourcen für Benutzeranwendungen frei.

Allerdings existiert eine Reihe von Programmen, die gestartet werden, wenn Prozessorressourcen frei werden, und im Hintergrundmodus arbeiten. Damit die Virenuntersuchung unabhängig von der Arbeit solcher Programme erfolgt, öffnen Sie das Konfigurationsfenster des Programms, wählen Sie den Abschnitt **Schutz** und deaktivieren Sie im Block **Erweitert** (s. Abb. 6) das Kontrollkästchen **Ressourcen für andere Anwendungen freigeben**.

Beachten Sie, dass dieser Parameter für jede Untersuchungsaufgabe individuell angepasst werden kann. In diesem Fall besitzt der für eine konkrete Aufgabe festgelegte Parameter die höchste Priorität.

6.5. Lösen von Kompatibilitätsproblemen von Kaspersky Anti-Virus mit anderen Anwendungen

In einigen Fällen können bei der Verwendung von Kaspersky Anti-Virus Konflikte bei der Arbeit mit Anwendungen, die auf dem Computer installiert sind, auftreten. Das steht mit dem in diese Programme integrierten Selbstschutzmechanismus in Verbindung, der reagiert, wenn Kaspersky Anti-Virus versucht, auf die Programme zuzugreifen. Zu diesen Programmen gehören beispielsweise das Plug-in Authentica des Programms Adobe Reader, das der Zugriffskontrolle für Dokumente im pdf-Format dient, das Programm zur Steuerung von Mobiltelefonen Oxygen Phone Manager II, sowie einige Arten von Spielen, die über einen Crackschutz verfügen.

Um dieses Problem zu lösen, öffnen Sie das Konfigurationsfenster des Programms, wählen Sie den Abschnitt **Schutz** und aktivieren Sie im Block **Kompatibilität** (s. Abb. 7) das Kontrollkästchen **Kompatibilität mit dem Selbstschutz von Programmen**. Damit die Änderungen dieses Parameters wirksam werden, ist der Neustart des Betriebssystems erforderlich.

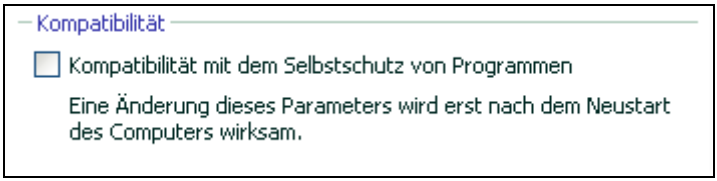

Kompatibilität
Kompatibilität mit dem Selbstschutz von Programmen
Eine Änderung dieses Parameters wird erst nach dem Neustart des Computers wirksam.

Abbildung 7. Kompatibilitätsparameter anpassen

Achtung!

Wenn die Anwendung auf einem Computer mit dem Betriebssystem Microsoft Windows Vista oder Microsoft Windows Vista x64 installiert ist, wird die Option zum Lösen von Kompatibilitätsproblemen mit dem Selbstschutz anderer Programme nicht unterstützt.

6.6. Start von Untersuchungs- und Update-Aufgaben mit Rechten eines anderen Benutzers

In Kaspersky Anti-Virus 7.0 ist ein Dienst zum Aufgabenstart unter einem anderen Benutzerkonto (Impersonalisierung) realisiert. Dieser Dienst ist standardmäßig deaktiviert und Aufgaben werden unter dem aktiven Benutzerkonto gestartet, mit dem Sie sich am System angemeldet haben.

Beispielsweise können beim Ausführen einer Untersuchungsaufgabe Zugriffsrechte für das zu untersuchende Objekt erforderlich sein. Dann können Sie diesen Dienst benutzen, um den Aufgabenstart unter dem Namen eines Benutzers zu starten, der über die erforderlichen Privilegien verfügt.

Das Programm-Update kann aus einer Quelle erfolgen, auf die Sie keinen Zugriff (beispielsweise ein Netzwerkverzeichnis für Updates) oder keine Rechte eines autorisierten Proxyserverbenutzers besitzen. In diesem Fall können Sie den Dienst benutzen, um das Programm-Update unter dem Namen eines Benutzers mit entsprechender Berechtigung zu starten.

Um den Start einer Untersuchungsaufgabe unter einem anderen Benutzerkonto festzulegen,

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie im Abschnitt **Virensuche** den Namen der Aufgabe.
2. Klicken Sie im Block **Sicherheitsstufe** auf die Schaltfläche **Einstellungen** und gehen Sie im folgenden Fenster auf die Registerkarte **Erweitert**.

Um den Start einer Update-Aufgabe unter einem anderen Benutzerkonto anzupassen,

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie den Abschnitt **Update**.

2. Klicken Sie im Block **Update-Einstellungen** auf die Schaltfläche **Einstellungen** und gehen Sie im folgenden Fenster auf die Registerkarte **Erweitert** (s. Abb. 8).

Aktivieren Sie das Kontrollkästchen ☑ **Aufgabenstart mit anderem Benutzernamen**, um diesen Dienst einzuschalten. Geben Sie darunter das Benutzerkonto an, unter dem die Aufgabe gestartet werden soll: Benutzername und Kennwort.

Hinweis

Beachten Sie, dass die zeitplangesteuerte Aktualisierung mit den Rechten des aktiven Benutzerkontos ausgeführt wird, wenn der Start mit Rechten eines anderen Benutzers nicht aktiviert wurde. Sollte es vorkommen, dass zu einem bestimmten Zeitpunkt kein Benutzer auf dem Computer angemeldet ist und der Updatestart nicht mit Rechten eines anderen Benutzers geplant wurde, dann wird das Update dem Zeitplan entsprechend mit den Rechten des Benutzers SYSTEM gestartet.

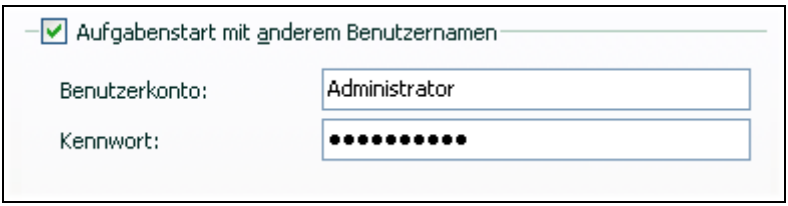


Abbildung 8. Einstellungen für den Start von Aufgaben unter einem anderen Benutzerkonto

6.7. Konfiguration des Zeitplans für Aufgabenstart und Senden von Benachrichtigungen

Die Konfiguration des Zeitplans ist für Aufgaben zur Virensuche, für das Anwendungsupdate und für das Senden von Benachrichtigungen über die Arbeit von Kaspersky Anti-Virus einheitlich.

Der Start der Aufgaben zur Virensuche, die bei der Anwendungsinstallation erstellt wurden, ist standardmäßig deaktiviert. Eine Ausnahme bildet die Untersuchungsaufgabe für Autostart-Objekte, die jedes Mal beim Start von Kaspersky Anti-Virus ausgeführt wird. Das Update wird in der Grundeinstellung automatisch ausgeführt, wenn auf den Kaspersky-Lab-Servern neue Updates vorhanden sind.

Sollten die Einstellungen für die Arbeit der Aufgaben nicht Ihren Anforderungen entsprechen, dann können Sie die Zeitplanparameter ändern.

Abbildung 9. Erstellen eines Zeitplans für den Aufgabenstart

Bestimmen Sie zuerst die Frequenz, mit der das betreffende Ereignis (Start einer Aufgabe oder Senden einer Benachrichtigung) ausgeführt werden soll. Wählen Sie dazu im Block **Frequenz** (s. Abb. 9) die gewünschte Variante. Geben Sie dann im Block **Zeitplaneinstellungen** die Parameter des Zeitplans für die gewählte Variante an. Folgende Varianten stehen zur Auswahl:

- **Einmal** – Der Start der Aufgabe oder das Senden einer Benachrichtigung erfolgt an dem angegebenen Tag zur festgelegten Uhrzeit.
- **Bei Programmstart** – Der Start der Aufgabe oder das Senden einer Benachrichtigung erfolgt jedes Mal, wenn Kaspersky Anti-Virus gestartet wird. Zusätzlich kann der Zeitraum nach dem Programmstart festgelegt werden, nach dessen Ablauf der Start ausgeführt werden soll.
- **Nach jedem Update** – Die Aufgabe wird nach jedem Update der Programm-Datenbanken gestartet (Dieser Punkt bezieht sich nur auf Untersuchungsaufgaben).
- **Minuten** – Das Zeitintervall zwischen den Aufgabenstarts oder dem Senden von Benachrichtigungen beträgt eine bestimmte Anzahl von Minuten. Geben Sie in den Zeitplaneinstellungen den Wert für das Intervall in Minuten an. Als Höchstwert gelten 59 Minuten.
- **Stunden** – Das Intervall zwischen den Aufgabenstarts oder dem Senden von Benachrichtigungen wird in Stunden festgelegt. Wenn Sie diese Frequenz

gewählt haben, geben Sie in den Zeitplaneinstellungen das Intervall **Alle n Stunden** an und bestimmen Sie das Intervall *n*. Wählen Sie beispielsweise für den stündlichen Start *Alle 1 Stunden*.

Tage – Der Aufgabestart oder das Senden von Benachrichtigungen wird im Intervall von einer bestimmten Anzahl von Tagen gestartet. Geben Sie in den Zeitplanparametern den Wert für das Intervall an:

- Wählen Sie die Variante **Alle n Tage** und geben Sie das Intervall *n* für die Anzahl der Tage an.
- Wählen Sie die Variante **Montag bis Freitag**, wenn der Start täglich von Montag bis Freitag erfolgen soll.
- Wählen Sie **Samstag + Sonntag**, damit der Start nur an Samstagen und Sonntagen erfolgt.

Geben Sie neben der Frequenz im Feld **Zeit** die Uhrzeit für den Start der Untersuchungsaufgabe an.

Wochen – Der Aufgabenstart oder das Senden von Benachrichtigungen erfolgt an bestimmten Wochentagen. Wenn Sie diese Frequenz gewählt haben, aktivieren Sie in den Zeitplaneinstellungen die Kontrollkästchen der Wochentage, an denen der Start ausgeführt werden soll. Geben Sie außerdem im Feld **Zeit** die Uhrzeit an.

Monate – Der Aufgabenstart oder das Senden von Benachrichtigungen wird einmal monatlich zum festgelegten Zeitpunkt ausgeführt.

Wenn der Start aus einem bestimmten Grund nicht möglich war (wenn beispielsweise kein Mailprogramm installiert oder der Computer zum betreffenden Zeitpunkt ausgeschaltet war), können Sie festlegen, dass die übersprungene Aufgabe automatisch gestartet wird, sobald dies möglich ist. Aktivieren Sie dazu im Zeitplanfenster das Kontrollkästchen ☑ **Übersprungene Aufgabe starten**.

6.8. Typen der zu kontrollierenden schädlichen Programme

Kaspersky Anti-Virus bietet Ihnen Schutz vor verschiedenen Arten schädlicher Programme. Unabhängig von den festgelegten Parametern schützt das Programm Ihren Computer stets vor den gefährlichsten Malware-Arten. Dazu zählen Viren, trojanische Programme und Hacker-Utilities. Diese Programme können Ihrem Computer ernsten Schaden zufügen. Um die Sicherheit des Computers zu erhöhen, können Sie die Liste der erkennbaren Bedrohungen erweitern. Aktivie-

ren Sie dazu die Kontrolle über unterschiedliche Arten potentiell gefährlicher Programme.

Um auszuwählen, vor welchen Arten schädlicher Programme Kaspersky Anti-Virus den Computer schützen soll, öffnen Sie das Konfigurationsfenster des Programms und wählen Sie den Abschnitt **Bedrohungen und Ausnahmen** (s. Abb. 10).

Die Bedrohungstypen (s. Pkt. 1.3 auf S. 12) werden im Block **Kategorien für schädliche Software** genannt:

- **Viren, Würmer, Trojaner**. Diese Gruppe umfasst die meistverbreiteten und gefährlichsten Kategorien schädlicher Programme. Der Schutz vor diesen Bedrohungen gewährleistet das minimal erforderliche Sicherheitsniveau. In Übereinstimmung mit den Empfehlungen der Kaspersky-Lab-Spezialisten kontrolliert Kaspersky Anti-Virus die schädlichen Programme dieser Kategorie immer.
- **Spyware, Adware, Dialer**. Diese Gruppe enthält potentiell gefährliche Software, die den Benutzer behindern oder dem Computer bedeutenden Schaden zufügen kann.
- **Potentiell gefährliche Software (Riskware)**. Diese Gruppe umfasst Programme, die nicht schädlich oder gefährlich sind, aber unter bestimmten Umständen benutzt werden können, um Ihrem Computer Schaden zuzufügen.

Die genannten Gruppen regulieren, in welchem Umfang die Programm-Datenbanken bei der Objektuntersuchung im Echtzeitschutz und bei der Virensuche auf Ihrem Computer verwendet werden.

Wenn alle Gruppen gewählt wurden, bietet Kaspersky Anti-Virus den maximalen Virenschutz Ihres Computers. Wenn die zweite und dritte Gruppe deaktiviert ist, schützt das Programm Sie nur vor den meistverbreiteten schädlichen Objekten. Dabei werden potentiell gefährliche und andere Programme nicht kontrolliert, die auf Ihrem Computer installiert werden können und durch ihre Aktionen Imageverlust und materiellen Schaden verursachen können.

Die Kaspersky-Lab-Spezialisten warnen davor, die Kontrolle der zweiten Gruppe zu deaktivieren. Sollte es vorkommen, dass Kaspersky Anti-Virus ein Programm als gefährlich klassifiziert, das Ihrer Meinung nach kein Risiko darstellt, wird empfohlen, es als Ausnahme festzulegen (s. Pkt. 6.9 auf S. 75).

Um die Typen der zu kontrollierenden schädlichen Programme auszuwählen,

öffnen Sie das Konfigurationsfenster des Programms und wählen Sie den Abschnitt **Bedrohungen und Ausnahmen**. Die Einstellungen erfolgen im Block **Kategorien für schädliche Software** (s. Abb. 10).

Kategorien für schädliche Software
Viren, Würmer, Trojaner und Hackerprogramme
Spyware, Adware, Dialer
Potentiell gefährliche Software (Riskware)
Ich bin damit einverstanden, dass bestimmte legale Programme als potentiell gefährlich eingestuft werden können, und möchte, dass sie auf dem Computer als Bedrohung gelten.

Abbildung 10. Auswahl der zu kontrollierenden Bedrohungstypen

6.9. Aufbau einer vertrauenswürdigen Zone

Die *vertrauenswürdige Zone* ist eine benutzerdefinierte Liste von Objekten, die das Programm Kaspersky Anti-Virus bei seiner Arbeit nicht kontrolliert. Mit anderen Worten ist dies eine Auswahl von Ausnahmen für den Schutz des Programms.

Die vertrauenswürdige Zone wird vom Benutzer unter Berücksichtigung der Besonderheiten von Objekten, mit denen er arbeitet, sowie von Programmen, die auf seinem Computer installiert sind, aufgebaut. Das Anlegen einer solchen Liste mit Ausnahmen kann beispielsweise erforderlich sein, wenn Kaspersky Anti-Virus den Zugriff auf ein bestimmtes Objekt oder Programm blockiert, Sie aber sicher sind, dass dieses Objekt bzw. Programm absolut unschädlich ist.

Von der Untersuchung können Dateien eines bestimmten Formats, Dateien nach Maske, bestimmte Bereiche (beispielsweise ein Ordner oder Programm) sowie Programmprozesse oder Objekte nach einem Bedrohungstyp gemäß der Klassifikation der Viren-Enzyklopädie (nach dem Status, der dem Objekt vom Programm bei der Untersuchung zugewiesen wurde) ausgeschlossen werden.

Hinweis

Ein ausgeschlossenes Objekt unterliegt nicht der Untersuchung, wenn das Laufwerk oder der Ordner untersucht wird, auf dem es sich befindet. Wird allerdings ein konkretes Objekt zur Untersuchung ausgewählt, dann wird die Ausnahmeregel ignoriert.

Um eine Liste von Ausnahmen für den Schutz zu erstellen,

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie den Abschnitt **Bedrohungen und Ausnahmen** (s. Abb. 10).

2. Klicken Sie im Block **Ausnahmen** auf die Schaltfläche **Vertrauenswürdige Zone**.

3. Konfigurieren Sie im folgenden Fenster (s. Abb. 11) die Ausnahmeregeln für Objekte und legen Sie die Liste der vertrauenswürdigen Anwendungen an.

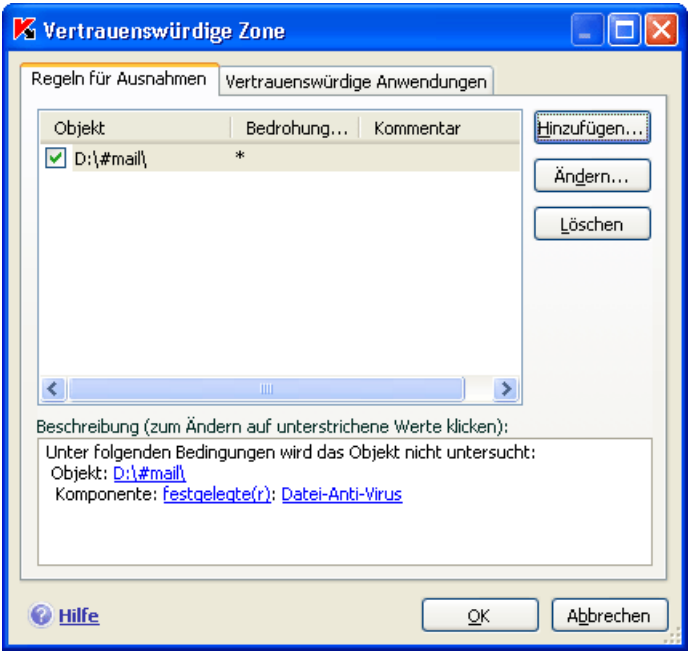


Abbildung 11. Erstellen der vertrauenswürdigen Zone

6.9.1. Ausnahmeregeln

Eine *Ausnahmeregel* ist eine Kombination von Bedingungen, bei deren Vorhandensein ein Objekt nicht von dem Programm Kaspersky Anti-Virus untersucht wird.

Von der Untersuchung können Dateien eines bestimmten Formats, Dateien nach Maske, bestimmte Bereiche (beispielsweise ein Ordner oder Programm) sowie Programmprozesse oder Objekte nach einem Bedrohungstyp gemäß der Klassifikation der Viren-Enzyklopädie ausgeschlossen werden.

Ein *Bedrohungstyp* ist ein Status, der einem Objekt bei der Untersuchung von der Anwendung Kaspersky Anti-Virus zugewiesen wird. Der Status beruht auf

der Klassifikation schädlicher und potentiell gefährlicher Programme, die in der Viren-Enzyklopädie von Kaspersky Lab enthalten ist.

Ein potentiell gefährliches Programm besitzt keine schädliche Funktion, kann aber von einem Schadprogramm als Hilfskomponente benutzt werden, weil es Schwachstellen und Fehler enthält. Zu dieser Kategorie gehören beispielsweise Programme zur entfernten Verwaltung, IRC-Clients, FTP-Server, alle Hilfsprogramme zum Beenden von Prozessen und zum Verstecken ihrer Arbeit, Tastaturspione, Programme zur Kennwortermittlung, Programme zur automatischen Einwahl auf kostenpflichtige Seiten usw. Solche Software wird nicht als Virus klassifiziert (not-a-virus), lässt sich aber beispielsweise in folgende Typen unterteilen: Adware, Joke, Riskware u.a. (ausführliche Informationen über potentiell gefährliche Programme, die von Kaspersky Anti-Virus entdeckt werden können, finden Sie in der Viren-Enzyklopädie auf der Seite www.viruslist.com/de). Derartige Programme können aufgrund der Untersuchung gesperrt werden. Da bestimmte Programme, die eine potentielle Gefahr darstellen, von vielen Benutzern verwendet werden, besteht die Möglichkeit, sie von der Untersuchung auszuschließen. Dazu muss der Name oder die Maske der Bedrohung nach der Klassifikation der Viren-Enzyklopädie zur vertrauenswürdigen Zone hinzugefügt werden.

Es kann beispielsweise sein, dass Sie häufig mit dem Programm Remote Administrator arbeiten. Dabei handelt es sich um ein System, das dem entfernten Zugriff dient und die Arbeit auf einem entfernten Computer erlaubt. Diese Anwendungsaktivität wird von Kaspersky Anti-Virus als potentiell gefährlich eingestuft und kann blockiert werden. Um zu verhindern, dass das Programm gesperrt wird, muss eine Ausnahmeregel erstellt werden, die den Bedrohungstyp not-a-virus:RemoteAdmin.Win32.RAdmin.22 enthält.

Beim Hinzufügen einer Ausnahme wird eine Regel erstellt, die danach für mehrere Programmkomponenten (Datei-Anti-Virus, Mail-Anti-Virus, Proaktiver Schutz, Web-Anti-Virus) sowie bei der Ausführung von Aufgaben zur Virensuche verwendet werden kann. Eine Ausnahmeregel kann entweder in dem dafür vorgesehenen Fenster erstellt werden, das aus dem Konfigurationsfenster des Programms geöffnet wird, oder aus der Meldung über den Fund eines Objekts, sowie aus dem Berichtsfenster.

*Hinzufügen einer Ausnahme zu den **Regeln für Ausnahmen**:*

1. Klicken Sie auf der Registerkarte **Regeln für Ausnahmen** auf die Schaltfläche **Hinzufügen** (s. Abb. 11.
2. Legen Sie im folgenden Fenster (s. Abb. 12) im Abschnitt **Parameter** den Typ der Ausnahme fest:

   Objekt – Ein bestimmtes Objekt, ein Ordner oder Dateien, die einer bestimmten Maske entsprechen, werden von der Untersuchung ausgeschlossen.

Bedrohungstyp – Ein Objekt wird von der Untersuchung ausgeschlossen, wobei sein Status entsprechend der Klassifikation der Viren-Enzyklopädie zugrunde gelegt wird.

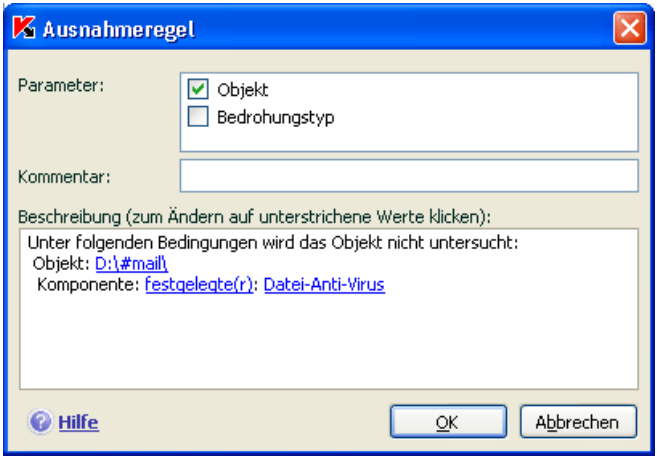


Abbildung 12. Erstellen einer Ausnahmeregel

Wenn gleichzeitig beide Kontrollkästchen angekreuzt werden, wird eine Regel für das angegebene Objekt mit einem bestimmten Bedrohungstyp nach der Klassifikation der Viren-Enzyklopädie erstellt. In diesem Fall gelten folgende Regeln:

- Wenn als **Objekt** eine bestimmte Datei festgelegt wird und als **Bedrohungstyp** ein bestimmter Status, dann wird die gewählte Datei nur dann ausgeschlossen, wenn ihr bei der Untersuchung der Status der festgelegten Bedrohung zugewiesen wurde.
- Wenn als **Objekt** ein bestimmter Bereich oder ein Ordner angegeben wird und als **Bedrohungstyp** ein Status (oder eine Maske), dann werden nur Objekte des gewählten Status von der Untersuchung ausgeschlossen, die im festgelegten Bereich bzw. Ordner gefunden wurden.

3. Legen Sie Werte für die gewählten Ausnahmetypen fest. Klicken Sie dazu im Abschnitt **Beschreibung** mit der linken Maustaste auf den Link angeben, der sich neben dem Typ der Ausnahme befindet:
   - Geben Sie für den Typ **Objekt** im folgenden Fenster den Namen des Objekts an (dabei kann es sich um eine Datei, einen Ordner oder eine Dateimaske handeln (s. Anhang A.2 auf S. 259). Aktivieren Sie das Kontrollkästchen **Unterordner einschließen**, damit das festgelegte Objekt (Datei, Dateimaske, Ordner) bei der Unter-

suchung rekursiv ausgeschlossen wird. Wenn Sie beispielsweise die Datei **C:\Programme\winword.exe** als Ausnahme festgelegt und das Kontrollkästchen für die Untersuchung von Unterordnern aktiviert haben, wird die Datei **winword.exe** von der Untersuchung ausgeschlossen, die sich in einem beliebigen Ordner des Verzeichnisses **C:\Programme** befinden kann.

- Geben Sie als **Bedrohungstyp** den vollständigen Namen der von der Untersuchung auszuschließenden Bedrohung an, wie er in der Viren-Enzyklopädie genannt wird, oder den Namen nach einer Maske (s. Anhang A.3 auf S. 260).

  Für einige Objekte, die nach Bedrohungstyp ausgeschlossen werden, können im Feld **Erweiterte Einstellungen** zusätzliche Bedingungen für die Verwendung der Regel festgelegt werden. In den meisten Fällen wird dieses Feld automatisch ausgefüllt, wenn eine Ausnahmeregel aus der Meldung des Proaktiven Schutzes hinzugefügt wird.

  Die Angabe von zusätzlichen Parametern kann beispielsweise für folgende Bedrohungen notwendig sein:

  - *Invader* (Eindringen in Programmprozesse). Für diese Bedrohung können Sie als zusätzliche Bedingung den Namen, die Maske oder den vollständigen Pfad des Zielobjekts angeben (z.B. der dll-Datei).
  - *Launching Internet Browser* (Browserstart mit Parametern) Für diese Bedrohung können Sie als zusätzliche Bedingung die Parameter für den Browserstart angeben. Beispielsweise haben Sie im Proaktiven Schutz bei der Aktivitätsanalyse von Anwendungen den Browserstart mit Parametern verboten, möchten aber als Ausnahmeregel den Browserstart für die Domäne *www.kasperky.com* mit einem Link aus Microsoft Office Outlook erlauben. Geben Sie dazu als **Objekt** der Ausnahme das Programm Microsoft Office Outlook, als **Bedrohungstyp** *Launching Internet Browser* und im Feld **Erweiterte Einstellungen** die Maske der erlaubten Domäne an.

4. Legen Sie fest, für welche Komponenten von Kaspersky Anti-Virus die neue Regel bei der Arbeit verwendet werden soll. Bei Auswahl des Werts jede(r) wird diese Regel für alle Komponenten übernommen. Wenn Sie die Verwendung der Regel auf eine oder mehrere Komponenten beschränken möchten, klicken Sie auf den Link jede(r). Der Link ändert sich in festgelegte. Durch Klick auf den Link angeben wird ein weiteres Fenster geöffnet. Aktivieren Sie dort die Kontrollkästchen der Komponenten, für welche diese Ausnahmeregel gelten soll.

Hinzufügen einer Ausnahmeregel aus der Programmmeldung über den Fund eines gefährlichen Objekts:

1. Verwenden Sie im Meldungsfenster (s. Abb. 13) den Link Zur vertrauenswürdigen Zone hinzufügen.
2. Überprüfen Sie im folgenden Fenster, ob alle Parameter der Ausnahmeregel korrekt sind. Die Felder mit dem Objektnamen und dem zugewiesenen Bedrohungstyp werden aufgrund der Informationen aus der Meldung automatisch ausgefüllt. Klicken Sie auf **OK**, um die Regel zu erstellen.

Datei-Anti-Virus
Datei enthält Potentiell gefährliche Software. Die Desinfektion ist nicht möglich Details...
Potentiell gefährliche Software:
not-a-virus:RemoteAdmin.Win32.RAdmin....
Datei:
D:\src\Kaspersky Anti-Virus 6.0...\raddrv.dll
Löschen
Datei wird gelöscht. Eine Kopie der Datei wird im Backup gespeichert.
Überspringen
Der Zugriff auf wird gesperrt. Datei wird nicht verändert oder gelöscht.
Zur vertrauenswürdigen Zone hinzufüg...
Für der Datei wird eine Ausnahmeregel erstellt.
In allen ähnlichen Fällen anwenden

Abbildung 13. Meldung über den Fund eines gefährlichen Objekts

Erstellen einer Ausnahmeregel vom Berichtsfenster aus:

1. Wählen Sie im Bericht das Objekt aus, das Sie zu den Ausnahmen hinzufügen möchten.
2. Öffnen Sie das Kontextmenü und wählen Sie den Punkt **Zur vertrauenswürdigen Zone hinzufügen** (s. Abb. 14).
3. Dadurch wird das Fenster zur Konfiguration der Ausnahme geöffnet. Überprüfen Sie, ob alle Parameter der Ausnahmeregel korrekt sind. Die Felder mit dem Objektnamen und dem zugewiesenen Bedrohungstyp

werden automatisch ausgefüllt, wozu Informationen aus dem Bericht dienen. Klicken Sie auf die Schaltfläche **OK**, um die Regel zu erstellen.

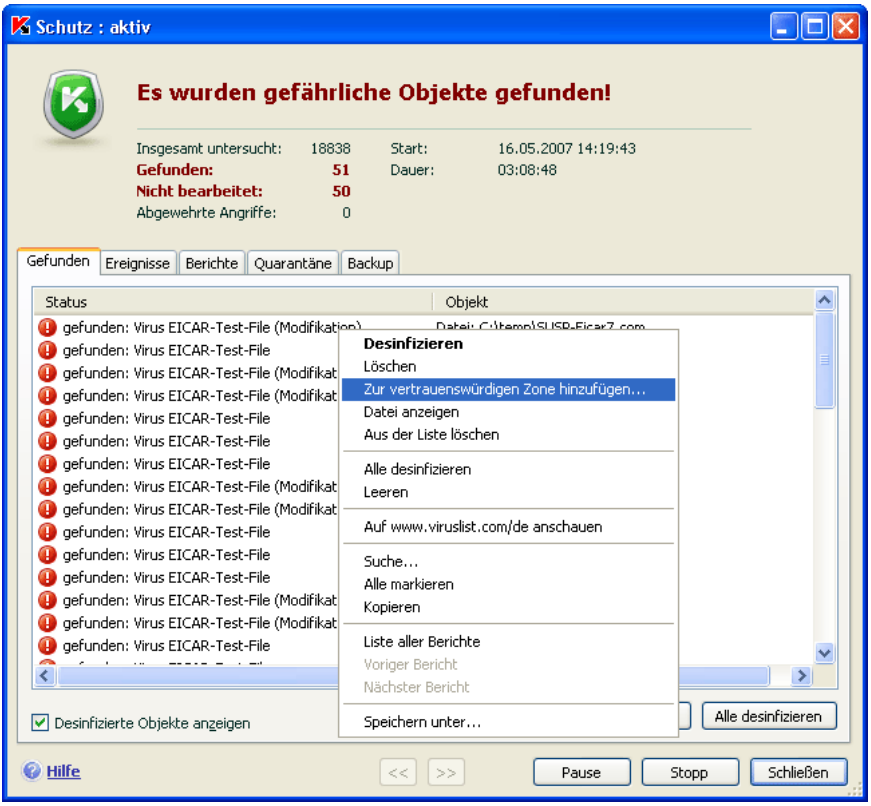


Abbildung 14. Erstellen einer Ausnahmeregel vom Bericht aus

6.9.2. Vertrauenswürdige Anwendungen

Kaspersky Anti-Virus erlaubt es, eine Liste von vertrauenswürdigen Anwendungen zu erstellen, deren Aktivität (einschließlich verdächtiger Aktivität, Datei- und Netzwerkaktivität sowie Zugriff auf die Systemregistrierung) nicht kontrolliert werden soll.

Wenn Sie beispielsweise die Objekte, die von dem standardmäßigen Microsoft Windows-Programm **Editor** verwendet werden, für ungefährlich und deren Untersuchung im Echtzeitschutz nicht für erforderlich halten, bedeutet das, dass Sie diesem Programm vertrauen. Um die Objekte, die von diesem Prozess benutzt

werden, von der Untersuchung auszuschließen, fügen Sie das Programm **Editor** zur Liste der vertrauenswürdigen Anwendungen hinzu. Trotzdem werden aber die ausführbare Datei und der Prozess einer vertrauenswürdigen Anwendung weiterhin auf Viren untersucht. Um eine Anwendung vollständig von der Untersuchung auszuschließen, müssen die Ausnahmeregeln verwendet werden (s. Pkt. 6.9.1 auf S. 76).

Einige Aktionen, die als gefährlich klassifiziert werden, sind im Rahmen der Funktionalität bestimmter Programme normal. Beispielsweise ist das Abfangen eines Texts, den Sie über die Tastatur eingeben, für Programme zum automatischen Umschalten der Tastaturbelegung (Punto Switcher u.ä.) eine normale Aktion. Um die Besonderheit solcher Programme zu berücksichtigen und die Kontrolle ihrer Aktivität abzuschalten, empfehlen wir, sie in die Liste der vertrauenswürdigen Anwendungen aufzunehmen.

Das Ausschließen vertrauenswürdiger Anwendungen aus der Untersuchung erlaubt es außerdem, mögliche Kompatibilitätsprobleme von Kaspersky Anti-Virus mit anderen Anwendungen zu lösen (wenn beispielsweise der Netzwerkverkehr von einem anderen Computer bereits von einer Antiviren-Anwendung untersucht wurde). Außerdem lässt sich auf diese Weise die Leistungsfähigkeit des Computers erhöhen, was insbesondere bei Serveranwendungen wichtig ist.

Kaspersky Anti-Virus untersucht standardmäßig alle Objekte, die von einem beliebigen Programmprozess geöffnet, gestartet oder gespeichert werden sollen, und kontrolliert die Aktivität aller Programme und den von ihnen erzeugten Netzwerkverkehr.

Die Liste der vertrauenswürdigen Anwendungen wird auf der Registerkarte **Vertrauenswürdige Anwendungen** erstellt (s. Abb. 15). Bei der Installation von Kaspersky Anti-Virus enthält die Liste der vertrauenswürdigen Anwendungen standardmäßig die Anwendungen, deren Aktivität aufgrund von Empfehlungen der Kaspersky-Lab-Spezialisten nicht analysiert wird. Wenn Sie eine in der Liste enthaltene Anwendung für nicht vertrauenswürdig halten, deaktivieren Sie das entsprechende Kontrollkästchen. Sie können die Liste mit Hilfe der rechts angebrachten Schaltflächen **Hinzufügen**, **Ändern** und **Löschen** bearbeiten.

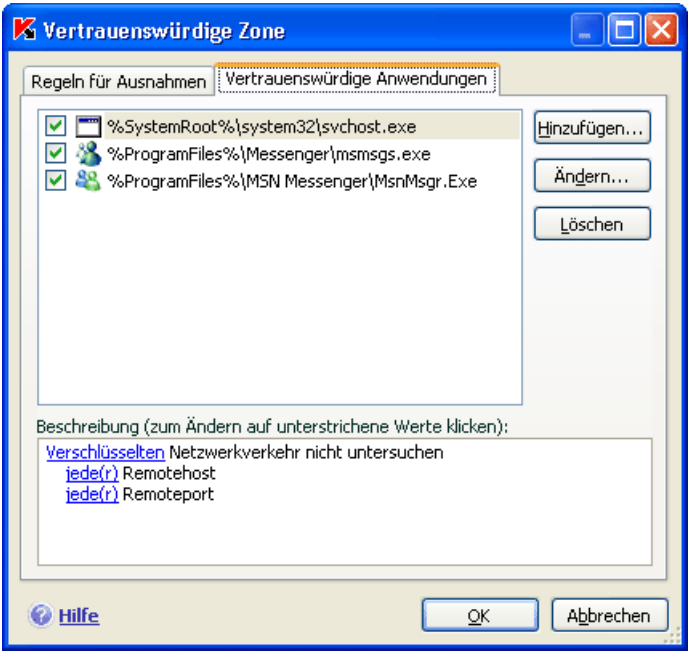


Abbildung 15. Liste der vertrauenswürdigen Anwendungen

Um ein Programm zur Liste der vertrauenswürdigen Anwendungen hinzuzufügen:

1. Klicken Sie auf die Schaltfläche **Hinzufügen**, die sich auf der rechten Seite der Registerkarte **Vertrauenswürdige Anwendungen** befindet.
2. Das Fenster **Vertrauenswürdige Anwendung** (s. Abb. 16) wird geöffnet. Klicken Sie zur Auswahl der Anwendung auf die Schaltfläche **Durchsuchen**. Dadurch öffnet sich ein Kontextmenü, in dem Sie mit dem Punkt **Durchsuchen** in das Standardfenster zur Dateiauswahl gelangen und den Pfad der ausführbaren Datei angeben können, oder mit dem Punkt **Anwendungen** zur Liste der momentan aktiven Anwendungen wechseln können, um die gewünschte auszuwählen.

   Bei der Auswahl eines Namens speichert Kaspersky Anti-Virus die internen Attribute der ausführbaren Datei, mit denen das Programm bei der Untersuchung als vertrauenswürdig identifiziert wird.

   Der Pfad der Datei wird bei der Auswahl des Namens automatisch ergänzt.

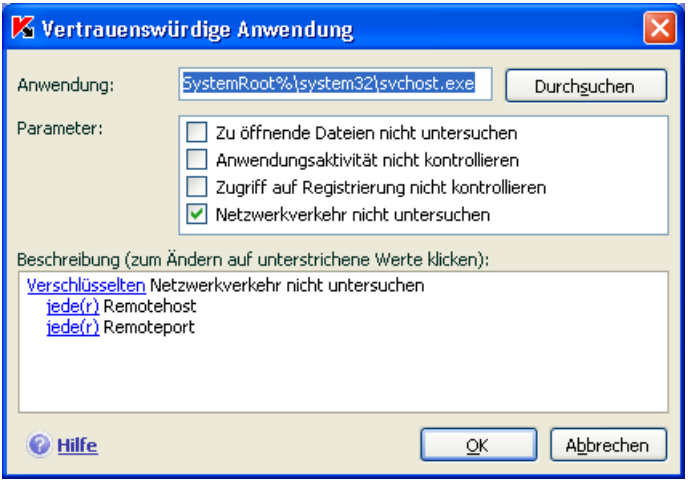


Abbildung 16. Hinzufügen einer Anwendung zur Liste der vertrauenswürdigen Anwendungen

3. Geben Sie nun die von diesem Prozess ausführbaren Aktionen an, die von Kaspersky Anti-Virus nicht kontrolliert werden sollen:

   - **Zu öffnende Dateien nicht untersuchen** – alle Dateien von der Untersuchung ausschließen, die von dem Prozess der vertrauenswürdigen Anwendung geöffnet werden.
   - **Anwendungsaktivität nicht kontrollieren** – Im Rahmen der Arbeit der Komponente Proaktiver Schutz soll jede beliebige Aktivität (einschließlich verdächtiger), die von der vertrauenswürdigen Anwendung ausgeführt wird, von der Untersuchung ausgeschlossen werden.
   - **Zugriff auf Registrierung nicht kontrollieren** – Die von vertrauenswürdigen Anwendungen initiierten Versuche zum Zugriff auf die Systemregistrierung werden von der Untersuchung ausgeschlossen.
   - **Netzwerkverkehr nicht untersuchen** – Den Netzwerkverkehr, der von einer vertrauenswürdigen Anwendung initiiert wird, aus der Viren- und Spam-Untersuchung ausschließen. Sie können entweder den gesamten Netzwerkverkehr einer Anwendung oder nur den (unter Verwendung des SSL-Protokolls) verschlüsselten Verkehr von der Untersuchung ausschließen. Klicken Sie dazu auf den Link Gesamten, der dann den Wert Verschlüsselten annimmt. Außerdem können Sie eine Ausnahme auf einen bestimmten Remotehost/Remoteport beschränken. Klicken Sie zur

Angabe der Beschränkung auf den Link jede(r), der sich dadurch in festgelegte(r) ändert, und geben Sie den Wert des Remotehosts bzw. Remoteports an.

KAPITEL 7. VIRENSCHUTZ FÜR DAS DATEISYSTEM DES COMPUTERS

Kaspersky Anti-Virus verfügt über eine spezielle Komponente, die das Dateisystem Ihres Computers vor einer Infektion schützt: *Datei-Anti-Virus*. Die Komponente wird beim Start des Betriebssystems gestartet, befindet sich ständig im Arbeitsspeicher des Computers und untersucht alle Dateien, , die geöffnet, gespeichert und gestartet werden.

Als Indikator für die Arbeit der Komponente dient das Symbol von Kaspersky Anti-Virus im Infobereich der Taskleiste von Microsoft Windows, das jedes Mal bei der Untersuchung einer Datei folgendes Aussehen annimmt .

Standardmäßig untersucht Datei-Anti-Virus *nur neue* oder *veränderte Dateien*, d.h. Dateien, die seit dem letzten Zugriff hinzugefügt oder verändert worden sind.

Die Dateiuntersuchung erfolgt nach folgendem Algorithmus:

1. Der Zugriff des Benutzers oder eines bestimmten Programms auf eine beliebige Datei wird von der Komponente abgefangen.
2. Datei-Anti-Virus überprüft, ob die Datenbanken iChecker™ und iSwift™ Informationen über die abgefangene Datei enthalten. Auf Grundlage der ermittelten Informationen wird über die Notwendigkeit der Dateiuntersuchung entschieden.

Der Untersuchungsvorgang umfasst folgende Schritte:

1. Die Datei wird auf das Vorhandensein von Viren untersucht. Schädliche Objekte werden auf Basis der *Programm-Datenbanken* erkannt. Die Datenbanken enthalten eine Beschreibung aller momentan bekannten Schadprogramme, Bedrohungen, Netzwerkangriffe und entsprechende Desinfektionsmethoden.
2. Aufgrund der Analyseergebnisse bestehen folgende Varianten für das weitere Vorgehen der Anwendung:
    a) Wenn in der Datei schädlicher Code gefunden wird, sperrt Datei-Anti-Virus die Datei und versucht, sie zu desinfizieren. Bei erfolgreicher Desinfektion wird die Datei zum Zugriff freigegeben. Wenn die Desinfektion fehlschlägt, wird die Datei gelöscht. Beim Desinfizieren oder Löschen der Datei wird eine Kopie der Datei im *Backup* gespeichert.

b) Wenn in der Datei ein Code gefunden wird, der Ähnlichkeit mit schädlichem Code besitzt, jedoch keine hundertprozentige Sicherheit darüber besteht, die Datei wird in den Quarantäne-Speicher verschoben. Es kann später versucht werden, sie mit aktualisierten Datenbanken zu desinfizieren.

c) Wenn in der Datei kein schädlicher Code gefunden wird, wird sie sofort zum Zugriff freigegeben.

7.1. Auswahl der Sicherheitsstufe für den Dateischutz

Datei-Anti-Virus bietet Schutz für die Dateien, mit denen Sie arbeiten. Dafür stehen folgende Sicherheitsstufen zur Auswahl (s. Abb. 17):

- **Maximaler Schutz** – Auf dieser Stufe erfolgt die Kontrolle über Dateien, die geöffnet, gespeichert und gestartet werden, mit maximaler Ausführlichkeit.
- **Empfohlen**. Die Parameter dieser Stufe werden von Kaspersky-Lab-Experten empfohlen und umfassen die Untersuchung folgender Objektkategorien:
  - Programm und Objekte nach ihrem Inhalt
  - nur neue und seit der letzten Objektuntersuchung veränderte Objekte
  - eingebettete OLE-Objekte
- **Maximales Tempo** – Diese Stufe erlaubt Ihnen, komfortabel mit Anwendungen zu arbeiten, die den Arbeitsspeicher stark beanspruchen, weil die Auswahl der untersuchten Dateien auf dieser Stufe eingeschränkt wird.

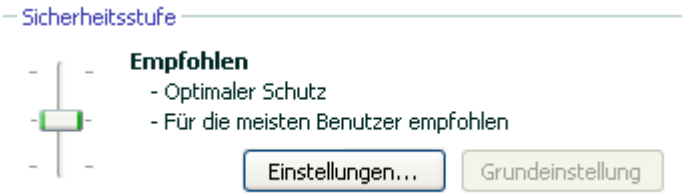


Abbildung 17. Sicherheitsstufe von Datei-Anti-Virus

Der Dateischutz erfolgt standardmäßig auf der **Empfohlenen** Stufe.

Sie können die Sicherheitsstufe für Dateien, mit denen Sie arbeiten, erhöhen oder senken, indem Sie eine andere Stufe wählen oder die Einstellungen der aktuellen Stufe ändern.

Um die Sicherheitsstufe zu ändern,

verschieben Sie den Zeiger auf der Skala. Durch das Anpassen der Sicherheitsstufe wird das Verhältnis zwischen der Ausführungsgeschwindigkeit der Untersuchung und der Anzahl der zu untersuchenden Dateien bestimmt: Je weniger Dateien der Virenanalyse unterzogen werden, desto höher ist die Untersuchungsgeschwindigkeit.

Wenn eine der vordefinierten Stufen für den Dateischutz nicht vollständig Ihren Anforderungen entspricht, können Sie die Schutzparameter zusätzlich anpassen. Wählen Sie dazu die Stufe, die Ihren Anforderungen am nächsten kommt, als Ausgangsstufe und ändern Sie ihre Parameter entsprechend. In diesem Fall ändert sich der Name der Stufe in **Benutzerdefiniert**. Betrachten wir ein Beispiel dafür, wann eine Änderung der vordefinierten Sicherheitsstufen nützlich sein kann.

Beispiel:

Aufgrund von Besonderheiten Ihrer Tätigkeit arbeiten Sie mit einer großen Menge von Dateien unterschiedlicher Typen, darunter auch relativ umfangreiche Dateien. Sie möchten es nicht riskieren, Dateien entsprechend der Namenserweiterung oder Größe von der Untersuchung auszuschließen, selbst wenn dadurch die Leistungsfähigkeit Ihres Computers beeinflusst wird.

Empfehlung zur Auswahl der Stufe:

Die Analyse der Situation lässt darauf schließen, dass die Infektionsgefahr durch ein Schadprogramm im beschriebenen Beispiel sehr groß ist. Größe und Typ von bei der Arbeit verwendeten Dateien sind sehr vielfältig, weshalb das Festlegen solcher Ausnahmen ein Risiko für die Daten auf dem Computer darstellt. Ein wichtiger Aspekt der Untersuchung besteht in der Analyse von bei der Arbeit verwendeten Dateien nach ihrem Inhalt und nicht nach der Erweiterung.

Es wird empfohlen, die vordefinierte Schutzstufe **Empfohlen** folgendermaßen anzupassen: Die Größenbeschränkung für zu untersuchende Dateien wird deaktiviert. Die Arbeit von Datei-Anti-Virus wird dadurch optimiert, dass nur neue und veränderte Dateien untersucht werden. Dadurch wird die Belastung des Computers bei der Dateiuntersuchung gesenkt, was die komfortable Arbeit mit anderen Anwendungen erlaubt.

Um die Einstellungen der aktuellen Sicherheitsstufe anzupassen,

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus**.
2. Klicken Sie im Block **Sicherheitsstufe** (s. Abb. 17) auf die Schaltfläche **Einstellungen**.
3. Passen Sie im folgenden Fenster die Parameter für den Dateischutz an und klicken Sie dann auf **OK**.

7.2. Konfiguration des Dateischutzes

Die Einstellungen, nach denen der Dateischutz auf Ihrem Computer erfolgt, lassen sich in folgende Gruppen aufteilen:

- Parameter, welche die Typen der Dateien festlegen, die der Virenanalyse unterzogen werden (s. Pkt. 7.2.1 auf S. 89).
- Parameter, die den geschützten Bereich festlegen (s. Pkt. 7.2.2 auf S. 92).
- Parameter, welche die Aktion für ein gefährliches Objekt festlegen (s. Pkt. 7.2.6 auf S. 101).
- Parameter, mit denen die Verwendung der heuristischen Analysemethoden festgelegt wird (s. Pkt. 7.2.4 auf S. 98)
- zusätzliche Parameter für die Arbeit von Datei-Anti-Virus (s. Pkt. 7.2.3 auf S. 95).

In diesem Abschnitt des Handbuchs werden alle oben genannten Gruppen ausführlich beschrieben.

7.2.1. Festlegen der Typen von zu untersuchenden Dateien

Durch die Angabe des Typs der zu untersuchenden Dateien definieren Sie das Format, die Größe und die Laufwerke der Dateien, die beim Öffnen, Ausführen und Speichern auf Viren untersucht werden sollen.

Zur Vereinfachung der Konfiguration werden alle Dateien in zwei Gruppen eingeteilt: *einfache* und *zusammengesetzte*. Einfache Dateien enthalten kein anderes Objekt (z.B. eine txt-Datei). Zusammengesetzte Objekte können mehrere Objekte umfassen, die wiederum jeweils mehrere Anhänge enthalten können. Hierfür

gibt es viele Beispiele: Archive, Dateien, die Makros, Tabellen, Nachrichten mit Anlagen usw. enthalten.

Der Dateityp für die Virenanalyse wird im Abschnitt **Dateitypen** (s. Abb. 18) festgelegt. Wählen Sie eine der drei Varianten:

- **Alle Dateien untersuchen**. In diesem Fall werden alle Objekte des Dateisystems, die geöffnet, gestartet und gespeichert werden ohne Ausnahmen der Analyse unterzogen.
- **Programme und Dokumente (nach Inhalt) untersuchen**. Bei der Auswahl dieser Dateigruppe untersucht Datei-Anti-Virus nur potentiell infizierbare Dateien, d.h. Dateien, in die ein Virus eindringen kann.

  Hinweis

  Es gibt eine Reihe von Dateiformaten, für die das Risiko des Eindringens von schädlichem Code und der späteren Aktivierung relativ gering ist. Dazu zählen beispielsweise Dateien im *txt*-Format.

  Im Gegensatz dazu gibt es Dateiformate, die ausführbaren Code enthalten oder enthalten können. Als Beispiele für solche Objekte dienen Dateien der Formate *exe*, *dll*, *doc*. Das Risiko des Eindringens und der Aktivierung von schädlichem Code ist für solche Dateien relativ hoch.

  Bevor die Virensuche in einer Datei beginnt, wird die interne Kopfzeile der Datei hinsichtlich des Dateiformats untersucht (txt, doc, exe usw.). Wenn sich aufgrund der Analyse ergibt, dass eine Datei dieses Formats nicht infiziert werden kann, dann wird sie nicht auf Viren untersucht und sofort für den Zugriff freigegeben. Besteht aber aufgrund des Dateiformats für einen Virus die Möglichkeit des Eindringens, dann wird die Datei auf Viren untersucht.

- **Programme und Dokumente (nach Erweiterung) untersuchen**. In diesem Fall untersucht Datei-Anti-Virus nur potentiell infizierbare Dateien, wobei das Format auf Basis der Dateinamenserweiterung ermittelt wird. Wenn Sie dem Link Erweiterung folgen, gelangen Sie zu einer Liste der Dateierweiterungen (s. Anhang A.1 auf S. 256), die in diesem Fall untersucht werden.

Hinweis

Es sollte beachtet werden, dass ein Angreifer einen Virus in einer Datei mit der Erweiterung txt an Ihren Computer senden kann, obwohl es sich in Wirklichkeit um eine ausführbare Datei handelt, die in eine txt-Datei umbenannt wurde. Wenn Sie die Variante **Programme und Dokumente (nach Erweiterung) untersuchen** wählen, wird eine solche Datei bei der Untersuchung übersprungen. Wenn Sie die Variante **Programme und Dokumente (nach Inhalt) untersuchen** gewählt haben, analysiert Datei-Anti-Virus ungeachtet der Erweiterung die Kopfzeile der Datei, wodurch sich ergibt, dass die Datei das Format exe besitzt. Eine solche Datei wird der sorgfältigen Virusuntersuchung unterzogen.

Abbildung 18. Auswahl der Dateitypen, die der Virenuntersuchung unterzogen werden sollen

Im Abschnitt **Optimierung** lässt sich festlegen, dass nur Dateien untersucht werden sollen, die neu sind oder seit ihrer letzten Untersuchung verändert wurden. Dieser Modus erlaubt es, die Untersuchungszeit wesentlich zu verkürzen und die Arbeitsgeschwindigkeit des Programms zu erhöhen. Aktivieren Sie dazu

das Kontrollkästchen **Nur neue und veränderte Dateien untersuchen**. Dieser Modus erstreckt sich auf gewöhnliche und zusammengesetzte Dateien.

Geben Sie im Abschnitt **Zusammengesetzte Dateien** an, welche zusammengesetzten Dateien auf Viren untersucht werden sollen:

- **Alle/Nur neue Archive untersuchen** – Archive der Formate ZIP, CAB, RAR, ARJ untersuchen.
- **Alle/Nur neue Installationspakete untersuchen** – selbstextrahierende Archive auf Viren untersuchen.
- **Alle/Nur neue angehängte(n) OLE-Objekte untersuchen** – Objekte, die in eine Datei eingebettet sind, untersuchen (z.B. eine Excel-Tabelle oder ein Makro, das in eine Datei des Typs Microsoft Office Word eingebettet ist, Anhänge von E-Mail-Nachrichten, usw.).

Für jeden Typ einer zusammengesetzten Datei können sie wählen, ob alle oder nur neue Dateien untersucht werden sollen. Verwenden Sie dazu den Link neben der Bezeichnung des Objekts. Der Link verändert seinen Wert, wenn mit der linken Maustaste darauf geklickt wird. Wenn im Abschnitt **Optimierung** festgelegt wurde, dass nur neue und veränderte Dateien untersucht werden sollen, steht die Auswahl des Typs der zusammengesetzten Dateien nicht zur Verfügung.

Um festzulegen, welche zusammengesetzten Dateien nicht auf Viren untersucht werden sollen, verwenden Sie folgende Parameter:

- **Später extrahieren, wenn Datei größer als ... MB**. Wenn die Größe eines zusammengesetzten Objekts diesen Wert überschreitet, wird es vom Programm wie ein einzelnes Objekt untersucht (Kopfzeile wird analysiert) und dem Benutzer zur Arbeit übergeben. Die Untersuchung der Objekte, die dazu gehören, erfolgt später. Wenn dieses Kontrollkästchen nicht aktiviert ist, wird der Zugriff auf Dateien, die über der angegebenen Größe liegen, bis zum Abschluss der Objektuntersuchung blockiert.
- **Nicht extrahieren, wenn Datei größer als ... MB**. In diesem Fall wird eine Datei mit der angegebenen Größe bei der Virenuntersuchung übersprungen.

7.2.2. Festlegen des Schutzbereichs

Datei-Anti-Virus untersucht standardmäßig alle Dateien, auf die zugegriffen wird, unabhängig davon, auf welchem Datenträger sie sich befinden (Festplatte, CD/DVD-ROM, Flash-Card).

Sie können den Schutzbereich folgendermaßen einschränken:

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus**.

2. Klicken Sie im Block **Sicherheitsstufe** (s. Abb. 17) auf die Schaltfläche **Einstellungen**.
3. Wählen Sie im folgenden Fenster die Registerkarte **Schutzbereich** (s. Abb. 19).

Auf der Registerkarte befindet sich eine Liste der Objekte, die der Untersuchung durch Datei-Anti-Virus unterliegen. Standardmäßig ist der Schutz aller Objekte aktiviert, die sich auf Festplatten, Wechseldatenträgern und Netzwerklaufwerken befinden, die an Ihren Computer angeschlossen sind. Sie können die Liste mit Hilfe der Schaltflächen **Hinzufügen**, **Ändern** und **Löschen** ergänzen oder anpassen.

Wenn Sie den Bereich der zu schützenden Objekte einschränken möchten, können Sie folgendermaßen vorgehen:

1. Nur die Verzeichnisse, Laufwerke oder Dateien angeben, die geschützt werden sollen.
2. Eine Liste der Objekte anlegen, die nicht geschützt werden sollen.
3. Die erste und zweite Methode vereinigen, d.h. einen Schutzbereich erstellen, aus dem bestimmte Objekte ausgeschlossen werden.

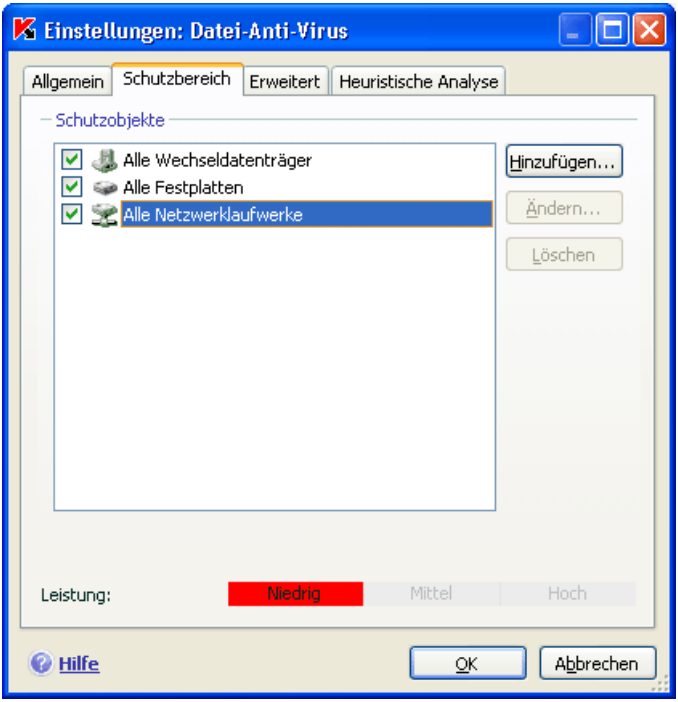


Abbildung 19. Festlegen des Schutzbereichs

Beim Hinzufügen eines Untersuchungsobjekts können Masken verwendet werden. Beachten Sie, dass Masken nur mit den absoluten Pfaden der Objekte angegeben werden dürfen:

- **C:\dir*.*** oder **C:\dir*** oder **C:\dir** – alle Dateien im Ordner *C:\dir*
- **C:\dir*.exe** – alle Dateien mit der Endung *.exe* im Ordner *C:\dir*
- **C:\dir*.ex?** – alle Dateien mit der Endung *.ex?* im Ordner *C:\dir*, wobei anstelle von ? ein beliebiges Zeichen stehen kann.
- **C:\dir\test** – nur die Datei *C:\dir\test*

Damit die rekursive Untersuchung des gewählten Objekts ausgeführt wird, aktivieren Sie das Kontrollkästchen ☑ **Unterordner einschließen**.

Achtung!

Beachten Sie, dass Datei-Anti-Virus nur jene Dateien auf Viren untersucht, die zu dem erstellten Schutzbereich gehören. Dateien, die nicht in diesen Bereich fallen, werden ohne Untersuchung zur Arbeit freigegeben. Dadurch steigt das Risiko einer Infektion Ihres Computers!

7.2.3. Anpassen zusätzlicher Parameter

Als zusätzliche Parameter für Datei-Anti-Virus können Sie den Untersuchungsmodus für die Objekte des Dateisystems festlegen und bestimmen, unter welchen Bedingungen die Arbeit der Komponente vorübergehend angehalten werden soll.

Um die zusätzlichen Parameter von Datei-Anti-Virus anzupassen:

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus**.
2. Klicken Sie im Block **Sicherheitsstufe** (s. Abb. 17) auf die Schaltfläche **Einstellungen**.
3. Wählen Sie im folgenden Fenster die Registerkarte **Erweitert** (s. Abb. 20).

Durch den Untersuchungsmodus für Objekte werden die Bedingungen für die Reaktion von Datei-Anti-Virus bestimmt. Folgende Varianten stehen zur Auswahl:

- **Intelligenter Modus**. Dieser Modus dient dazu, die Objektbearbeitung und die Verfügbarkeit von Objekten für den Benutzer zu beschleunigen. Bei der Auswahl dieser Variante wird aufgrund der Analyse der Operationen, die mit einem Objekt ausgeführt werden sollen, über die Untersuchung entschieden.

  Bei der Arbeit mit einem Microsoft Office-Dokument untersucht Kaspersky Anti-Virus die Datei, wenn sie zum ersten Mal geöffnet und zum letzten Mal geschlossen wird. Alle dazwischen liegenden Operationen, bei denen die Datei verändert wird, werden von der Untersuchung ausgeschlossen.

  Der intelligente Untersuchungsmodus wird standardmäßig verwendet.

- **Beim Öffnen und Ändern** – Datei-Anti-Virus untersucht Objekte, wenn sie geöffnet und verändert werden.
- **Beim Öffnen** – Objekte werden nur untersucht, wenn versucht wird, sie zu öffnen.

- **Bei Ausführung** – Objekte werden nur in dem Moment untersucht, wenn versucht wird, sie zu starten.

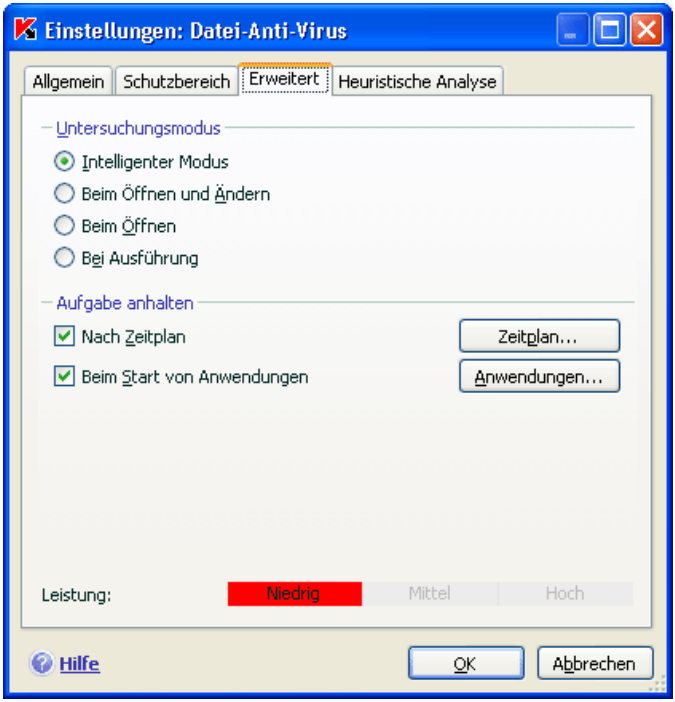


Abbildung 20. Anpassen der zusätzlichen Parameter für Datei-Anti-Virus

Das vorübergehende Anhalten von Datei-Anti-Virus kann erforderlich sein, wenn Arbeiten ausgeführt werden, die die Betriebssystemressourcen stark beanspruchen. Um die Belastung zu verringern und den schnellen Zugriff des Benutzers auf Objekte zu gewährleisten, wird empfohlen, das Abschalten der Komponente für einen bestimmten Zeitraum oder bei der Arbeit mit bestimmten Programmen festzulegen.

Damit die Arbeit der Komponente für einen bestimmten Zeitraum angehalten wird, aktivieren Sie das Kontrollkästchen ☑ **Nach Zeitplan** und legen Sie im Fenster (s. Abb. 21) das mit der Schaltfläche **Zeitplan** geöffnet wird, den Zeitraum fest, für den die Arbeit der Komponente angehalten und nach dem sie fortgesetzt werden soll. Geben Sie in den entsprechenden Feldern die Werte im Format HH:MM ein.

Abbildung 21. Die Arbeit der Komponente anhalten

Damit die Arbeit der Komponente bei der Arbeit mit ressourcenaufwändigen Programmen angehalten wird, aktivieren Sie das Kontrollkästchen **Beim Start von Anwendungen** und legen Sie im Fenster (s. Abb. 22), das mit der Schaltfläche **Liste** geöffnet wird, die Liste der Programme an.

Verwenden Sie die Schaltfläche **Hinzufügen**, um der Liste eine Anwendung hinzuzufügen. Dadurch wird das Kontextmenü geöffnet. Wechseln Sie entweder mit dem Punkt **Durchsuchen** in das Standardfenster zur Dateiauswahl und geben Sie die ausführbare Datei der betreffenden Anwendung an oder verwenden Sie den Punkt **Anwendungen**, um zur Liste der momentan aktiven Anwendungen zu gelangen, und wählen Sie dort die gewünschte Anwendung aus.

Um eine Anwendung aus der Liste zu löschen, wählen Sie sie in der Liste aus und klicken Sie auf die Schaltfläche **Löschen**.

Um eine Bedingung für das Anhalten von Datei-Anti-Virus bei der Arbeit einer konkreten Anwendung vorübergehend aufzuheben, ist es ausreichend, das Kontrollkästchen neben dem Namen der Anwendung zu deaktivieren, ohne diese aus der Liste zu löschen.

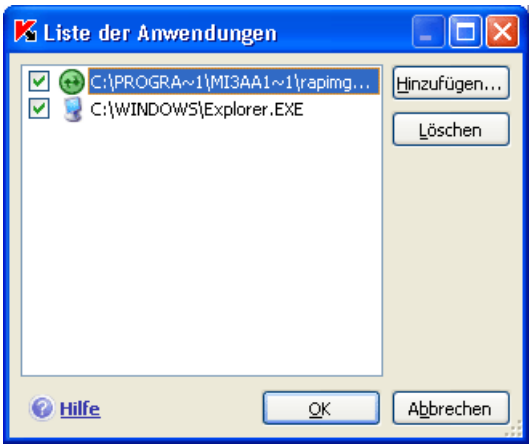


Abbildung 22. Liste der Anwendungen erstellen

7.2.4. Verwendung von heuristischen Analysemethoden

Heuristische Analysemethoden werden bei der Arbeit bestimmter Echtzeitschutz-Komponenten (z.B. für Datei-Anti-Virus, Mail-Anti-Virus und Web-Anti-Virus) und bei Aufgaben zur Virensuche verwendet.

Es ist bekannt, dass die Untersuchung mit der Signaturmethode mit zuvor erstellten Datenbanken, die eine Beschreibung bekannter Bedrohungen und entsprechende Desinfektionsmethoden enthalten, eine eindeutige Antwort darauf gibt, ob das untersuchte Objekte schädlich ist und zu welcher Klasse von Schadprogrammen es gegebenenfalls gehört. Im Unterschied zur Signaturmethode orientiert sich die heuristische Methode bei der Suche nach Bedrohungen nicht an Malware-Signaturen, sondern an typischen Operationsfolgen, die mit hinreichender Wahrscheinlichkeit eine Schlussfolgerung über die Art einer Datei zulassen. Der Vorteil der heuristischen Analyse besteht darin, dass für ihre Arbeit keine zuvor erstellten Datenbanken benötigt werden. Dadurch können neue Bedrohungen bereits erkannt werden, bevor die Virenanalytiker von ihrer Aktivität wissen.

Der heuristische Analysator emuliert die Ausführung des Objekts in einer ungefährlichen virtuellen Umgebung von Kaspersky Anti-Virus. Wenn das Verhalten des Objektes unverdächtig ist, wird dessen Ausführung in der Arbeitsumgebung zugelassen. Wenn bei der Ausführung verdächtige Aktionen erkannt werden, wird das Objekt als schädlich eingestuft. Der Start des Objekts

wird auf dem Computer gesperrt oder der Benutzer wird nach den weiteren Aktionen gefragt:

- Die Bedrohung in die Quarantäne verschieben, um sie später mit Hilfe aktualisierter Datenbanken zu untersuchen und zu bearbeiten.
- Das Objekt löschen.
- Überspringen, wenn Sie absolut sicher sind, dass das Objekt unschädlich ist.

Um die heuristischen Methoden zu verwenden, aktivieren Sie das Kontrollkästchen **Heuristische Analyse verwenden**. Sie können zusätzlich die Genauigkeitsstufe der Untersuchung anpassen. Bewegen Sie dazu den Schieberegler auf die gewünschte Position: **Oberflächlich**, **Mittel** oder **Detailliert**. Durch die Genauigkeitsstufe lässt sich das Verhältnis von Ausführlichkeit und damit Qualität der Suche nach neuen Bedrohungen zu dem Auslastungsniveau der Systemressourcen und der Untersuchungsdauer regulieren. Je höher die Genauigkeitsstufe der heuristischen Analyse, desto mehr Systemressourcen sind für die Untersuchung erforderlich und desto länger dauert der Vorgang.

Achtung!

Die Kaspersky-Lab-Spezialisten analysieren neue Bedrohungen, die mit Hilfe der heuristischen Analyse gefunden werden, umgehend und fügen den im Stundenrhythmus erscheinenden Programm-Datenbanken entsprechende Desinfektionsmethoden zu hinzu.

Wenn Sie die Programm-Datenbanken regelmäßig aktualisieren und die optimale Schutzstufe des Computers gewährleisten, ist es deshalb nicht notwendig, die heuristischen Analysemethoden permanent zu verwenden.

Auf der Registerkarte **Heuristische Analyse** (s. Abb. 23) können Sie die Verwendung von heuristischen Methoden zur Suche neuer Bedrohungen bei der Arbeit der Komponente Datei-Anti-Virus aktivieren/deaktivieren. Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus**.
2. Klicken Sie im Block **Sicherheitsstufe** (s. Abb. 17) auf die Schaltfläche **Einstellungen**.
3. Wählen Sie im folgenden Fenster die Registerkarte **Heuristische Analyse**.

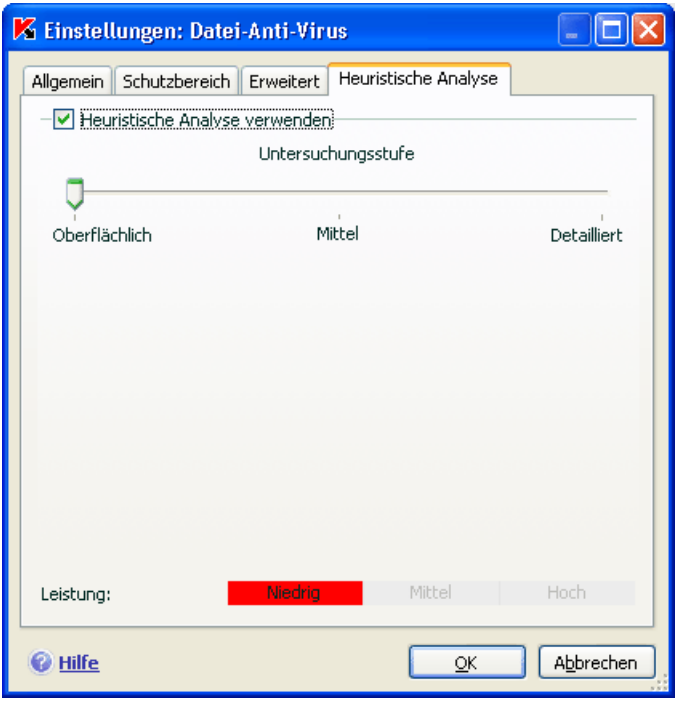


Abbildung 23. Verwendung von heuristischen Analysemethoden

7.2.5. Wiederherstellen der Standardparameter für den Dateischutz

Während Sie die Arbeit von Datei-Anti-Virus konfigurieren, können Sie jederzeit zu den empfohlenen Einstellungen zurückkehren. Diese gelten als optimal, werden von den Kaspersky-Lab-Spezialisten empfohlen und sind in der Sicherheitsstufe **Empfohlen** zusammengefasst.

Um die standardmäßigen Einstellungen für den Dateischutz wiederherzustellen,

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus**.
2. Klicken Sie im Block **Sicherheitsstufe** (s. Abb. 17) auf die Schaltfläche **Grundeinstellung**.

Wenn Sie bei der Konfiguration von Datei-Anti-Virus die Liste der Objekte verändert haben, die zum Schutzbereich gehören, wird Ihnen beim Wiederherstellen der ursprünglichen Einstellungen vorgeschlagen, diese Liste zur späteren Verwendung zu speichern. Um die Liste der Objekte beizubehalten, aktivieren Sie im folgenden Fenster **Einstellungen wiederherstellen** das ☑ Kontrollkästchen **Schutzbereich**.

7.2.6. Auswahl der Aktion für Objekte

Wenn sich durch die Virenuntersuchung einer Datei herausstellt, dass sie infiziert oder einer Infektion verdächtig ist, hängen die weiteren Operationen von Datei-Anti-Virus vom Status des Objekts und der ausgewählten Aktion ab.

Datei-Anti-Virus kann einem Objekt aufgrund der Untersuchung einen der folgenden Status zuweisen:

- Status eines der schädlichen Programme (beispielsweise *Virus*, *trojanisches Programm*) (s. Pkt. 1.3 auf S. 12).
- *möglicherweise infiziert*, wenn sich aufgrund der Untersuchung nicht eindeutig feststellen lässt, ob das Objekt infiziert ist oder nicht. Das bedeutet, dass in der Datei die Codefolge eines unbekannten Virus oder der modifizierte Code eines bekannten Virus gefunden wurde.

Standardmäßig werden alle infizierten Dateien der Desinfektion unterzogen. Alle möglicherweise infizierten Dateien werden in die Quarantäne verschoben.

Um die Aktion für ein Objekt zu ändern,

öffnen Sie das Konfigurationsfenster des Programms und wählen Sie im Abschnitt **Schutz** die Komponente **Datei-Anti-Virus**. Alle verfügbaren Aktionen sind im entsprechenden Abschnitt angegeben (s. Abb. 24).

Abbildung 24. Mögliche Aktionen von Datei-Anti-Virus für ein gefährliches Objekt

Gewählte Aktion	**Was geschieht beim Fund eines gefährlichen Objekts?**
◉ **Aktion erfragen**	Datei-Anti-Virus zeigt auf dem Bildschirm eine Warnmeldung an, die dar-

Gewählte Aktion	Was geschieht beim Fund eines gefährlichen Objekts?
	über informiert, von welchem schädlichen Objekt die Datei infiziert bzw. möglicherweise infiziert ist, und bietet Aktionen zur Auswahl an. Die Aktionen können abhängig vom Objektstatus variieren.
Zugriff verweigern	Datei-Anti-Virus blockiert den Zugriff auf das Objekt. Informationen darüber werden im Bericht (s. Pkt. 15.3 auf S. 195) aufgezeichnet. Später kann versucht werden, das Objekt zu desinfizieren.
Zugriff verweigern **Desinfizieren**	Datei-Anti-Virus blockiert den Zugriff auf das Objekt und versucht es zu desinfizieren. Wenn das Objekt nicht desinfiziert werden kann, erhält es den Status *möglicherweise infiziert* und wird in die Quarantäne verschoben (s. Pkt. 15.1 auf S. 188). Informationen darüber werden im Bericht zeichnet. Später kann versucht werden, dieses Objekt zu desinfizieren.
Zugriff verweigern **Desinfizieren** **Löschen, wenn Desinfektion nicht möglich**	Datei-Anti-Virus blockiert den Zugriff auf das Objekt und versucht, es zu desinfizieren. Wenn die Desinfektion des Objekts gelingt, wird der Zugriff freigegeben. Wenn das Objekt nicht desinfiziert werden kann, wird es löscht. Dabei wird eine Kopie des Objekts im Backup (s. Pkt. 15.2 auf S. 193) abgelegt.
Zugriff verweigern **Löschen**	Datei-Anti-Virus blockiert den Zugriff auf das Objekt und löscht es.

Bevor ein Desinfektionsversuch erfolgt oder das Objekt gelöscht wird, legt Kaspersky Anti-Virus eine Sicherungskopie des Objekts an und speichert diese im

Backup. Dadurch wird erlaubt, das Objekt bei Bedarf wiederherzustellen oder später zu desinfizieren.

7.3. Aufgeschobene Desinfektion von Objekten

Wenn Sie als Aktion für schädliche Objekte **Zugriff verweigern** gewählt haben, dann erfolgt für diese keine Desinfektion und der Zugriff wird gesperrt.

Wenn Sie als Aktion

Zugriff verweigern

Desinfizieren

gewählt haben, dann werden alle Objekte, deren Desinfektion nicht möglich ist, gesperrt.

Um erneut Zugriff auf blockierte Objekte zu erhalten, müssen diese vorher desinfiziert werden. Dazu:

1. Wählen Sie im Abschnitt **Schutz** des Programmhauptfensters die Komponente **Datei-Anti-Virus** und verwenden Sie den Link Bericht öffnen.
2. Wählen Sie auf der Registerkarte **Gefunden** die gewünschten Objekte und klicken Sie auf die Schaltfläche **Aktionen → Alle desinfizieren**.

Wenn die Desinfektion des Objekts gelingt, wird der Zugriff darauf freigegeben. Kann das Objekt nicht desinfiziert werden, dann wird Ihnen zur Auswahl angeboten, es zu *löschen* oder zu *überspringen*. Beim Überspringen wird die Datei für den Zugriff freigegeben. Allerdings erhöht sich dadurch das Risiko einer Infektion Ihres Computers erheblich. Es wird ausdrücklich davor gewarnt, schädliche Objekte zu überspringen.

KAPITEL 8. E-MAIL-VIRENSCHUTZ

Kaspersky Anti-Virus enthält eine spezielle Komponente, die den Schutz der ein- und ausgehenden E-Mail vor gefährlichen Objekten gewährleistet: *Mail-Anti-Virus.* Diese Komponente wird beim Start des Betriebssystems gestartet, befindet sich ständig im Arbeitsspeicher des Computers und untersucht alle E-Mails der Protokolle POP3, SMTP, IMAP, MAPI[1] und NNTP, sowie über geschützte Verbindungen (SSL) mit den Protokollen POP3 und IMAP.

Als Indikator für die Arbeit der Komponente dient das Symbol von Kaspersky Anti-Virus im Infobereich der Taskleiste von Microsoft Windows, das jedes Mal bei der Untersuchung einer E-Mail folgendes Aussehen annimmt: .

Der E-Mail-Schutz erfolgt standardmäßig nach folgendem Algorithmus:

1. Jeder Brief, der vom Benutzer empfangen oder gesendet wird, wird von Mail-Anti-Virus abgefangen.
2. Die E-Mail-Nachricht wird in ihre Bestandteile zerlegt: Kopfzeile, Briefkörper, Anhänge.
3. Der Körper und die Anhänge der E-Mail-Nachricht (einschließlich eingebetteter OLE-Objekte) werden auf gefährliche Objekte untersucht. Die Suche nach schädlichen Objekten erfolgt auf Basis der *Datenbanken*, die bei der Arbeit des Programms verwendet werden, sowie mit Hilfe eines heuristischen Algorithmus. Die Datenbanken enthalten eine Beschreibung aller momentan bekannten schädlichen Programme und Methoden zu deren Desinfektion. Der heuristische Algorithmus erlaubt es, neue Viren zu erkennen, die noch nicht in den Datenbanken beschrieben sind.
4. Aufgrund der Virenuntersuchung bestehen folgende Varianten für das weitere Vorgehen:
   - Wenn der Körper oder ein Anhang der Nachricht schädlichen Code enthält, sperrt Mail-Anti-Virus den Brief, speichert eine Kopie des infizierten Objekts im *Backup* und versucht das Objekt zu desinfi-

[1] Die Untersuchung von E-Mails des MAPI-Protokolls wird mit Hilfe eines speziellen Erweiterungsmoduls in Microsoft Office Outlook und The Bat! ausgeführt.

zieren. Bei erfolgreicher Desinfektion wird dem Benutzer der Zugriff auf den Brief freigegeben. Wenn die Desinfektion fehlschlägt, wird das infizierte Objekt aus dem Brief gelöscht. Zudem wird in die Betreffzeile des Briefs ein spezieller Text eingefügt, der darüber informiert, dass der Brief von Kaspersky Anti-Virus bearbeitet wurde.

- Wenn der Körper oder ein Anhang der Nachricht einen Code enthält, der Ähnlichkeit mit schädlichem Code besitzt, jedoch keine hundertprozentige Sicherheit darüber besteht, wird der verdächtige Teil des Briefs in den *Quarantäne-Speicher* verschoben.
- Wenn im Brief kein schädlicher Code gefunden wird, erhält der Benutzer sofort Zugriff darauf.

Für das Mailprogramm Microsoft Office Outlook ist ein spezielles integriertes Erweiterungsmodul vorgesehen (s. Pkt. 8.2.2 auf S. 110), das die Feineinstellung der E-Mail-Untersuchung erlaubt.

Wenn Sie das Mailprogramm The Bat! verwenden, kann Kaspersky Anti-Virus zusammen mit anderen Antiviren-Anwendungen benutzt werden. Dabei werden die Regeln zur Bearbeitung des Mailverkehrs (s. Pkt. 8.2.3 auf S. 112) direkt im Programm The Bat! erstellt und besitzen Vorrang gegenüber den Parametern für den E-Mail-Schutz durch Kaspersky Anti-Virus.

Bei der Arbeit mit anderen Mailprogrammen (einschließlich Microsoft Outlook Express (Windows Mail), Mozilla Thunderbird, Eudora, Incredimail) untersucht Mail-Anti-Virus den Mailverkehr der Protokolle SMTP, POP3, IMAP und NNTP bei Empfang bzw. Versand.

Achtung!

Beachten Sie, dass bei der Arbeit mit dem Mailprogramm Thunderbird E-Mails des Protokolls IMAP nicht auf Viren untersucht werden, wenn Filter verwendet werden, welche die Nachrichten aus dem Ordner **Inbox** verschieben.

8.1. Auswahl der E-Mail-Sicherheitsstufe

Kaspersky Anti-Virus bietet den Schutz Ihrer Post auf einer der folgenden Stufen (s. Abb. 25):

Maximaler Schutz – Auf dieser Stufe erfolgt die Kontrolle über ein- und ausgehende E-Mail-Nachrichten mit maximaler Ausführlichkeit. Das Programm untersucht unabhängig von der Untersuchungszeit ausführlich die an Briefe angehängten Objekte, einschließlich Archiven.

Empfohlen – Die Parameter dieser Stufe entsprechen den von Kaspersky-Lab-Experten empfohlenen Einstellungen. Sie umfassen die Untersuchung der gleichen Objekte wie auf der Stufe **Maximaler Schutz** unter Ausnahme von angehängten Objekten oder Briefen, deren Untersuchung länger als drei Minuten dauert.

Maximales Tempo – Diese Sicherheitsstufe erlaubt Ihnen, komfortabel mit Anwendungen zu arbeiten, die den Arbeitsspeicher stark beanspruchen, weil die Auswahl der untersuchten E-Mail-Objekte auf dieser Stufe eingeschränkt wird. Auf dieser Stufe wird nur Ihre eingehende Post untersucht, wobei angehängte Archive und Objekte (Briefe), deren Untersuchung länger als drei Minuten dauert, nicht untersucht werden. Es wird empfohlen, diese Stufe zu verwenden, wenn auf dem Computer zusätzliche Mittel zum E-Mail-Schutz installiert sind.

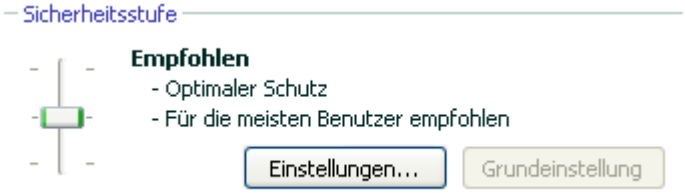


Abbildung 25. Auswahl der Sicherheitsstufe für Mail-Anti-Virus

Der E-Mail-Schutz arbeitet standardmäßig auf der **Empfohlenen** Stufe.

Sie können die Schutzstufe für Ihre Post erhöhen oder senken, indem Sie eine andere Stufe wählen oder die Einstellungen der aktuellen Stufe ändern.

Um die Sicherheitsstufe zu ändern,

verschieben Sie den Zeiger auf der Skala. Durch das Anpassen der Sicherheitsstufe wird das Verhältnis zwischen der Ausführungsgeschwindigkeit der Untersuchung und der Anzahl der zu untersuchenden Objekte bestimmt: Je weniger E-Mail-Objekte der Analyse auf gefährliche Objekte unterzogen werden, desto höher ist die Untersuchungsgeschwindigkeit.

Wenn eine vordefinierte Stufe nicht vollständig Ihren Anforderungen entspricht, können Sie die Parameter zusätzlich anpassen. Wählen Sie dazu die Stufe, die Ihren Anforderungen am nächsten kommt, als Ausgangsstufe und ändern Sie ihre Parameter entsprechend. In diesem Fall ändert sich der Name der Stufe in **Benutzerdefiniert**. Betrachten wir ein Beispiel dafür, wann eine Änderung der vordefinierten Sicherheitsstufen nützlich sein kann.

Beispiel:

Ihr Computer befindet sich in einem lokalen Netzwerk und die Internetverbindung erfolgt über ein Modem. Als Mailprogramm zum Empfang und Versand der E-Mail-Korrespondenz wird Microsoft Outlook Express verwendet. Sie verwenden einen kostenlosen E-Mail-Anbieter. Ihre Post enthält aus gewissen Gründen häufig angehängte Archive. Wie lässt sich Ihr Computer optimal vor einer per E-Mail übertragenen Infektion schützen?

Empfehlung zur Auswahl der Stufe:

Die Analyse der Situation lässt darauf schließen, dass die Infektionsgefahr durch ein per E-Mail übertragenes Schadprogramm im beschriebenen Beispiel sehr groß ist (Fehlen eines zentralen E-Mail-Schutzes und Verbindungsmethode zum Internet).

Es wird empfohlen, die vordefinierte Sicherheitsstufe **Maximaler Schutz** mit folgenden Änderungen zu verwenden: Die Untersuchungszeit für angehängte Objekte wird auf 1-2 Minuten verkürzt. Die Mehrzahl der angehängten Archive wird auf Viren untersucht und die E-Mail-Bearbeitung wird unwesentlich verlangsamt.

Um die Einstellungen der aktuellen Sicherheitsstufe anzupassen,

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie im Abschnitt Schutz die Komponente **Mail-Anti-Virus**.
2. Klicken Sie im Block **Sicherheitsstufe** (s. Abb. 25) auf die Schaltfläche **Einstellungen**.
3. Passen Sie im folgenden Fenster die Parameter für den Mail-Schutz an und klicken Sie dann auf **OK**.

8.2. Konfiguration des E-Mail-Schutzes

Die Regeln, nach denen die Untersuchung Ihrer Post erfolgt, werden durch eine Anzahl von Parametern bestimmt. Sie lassen sich in folgende Gruppen aufteilen:

- Parameter, welche die geschützte Richtung der Nachrichten bestimmen (s. Pkt. 8.2.1 auf S. 108).
- Parameter, mit denen die Verwendung der heuristischen Analysemethoden festgelegt wird (s. Pkt. 8.2.4 auf S. 114).
- Parameter für die E-Mail-Untersuchung in Microsoft Office Outlook (s. Pkt. 8.2.2 auf S. 110) und The Bat! (s. Pkt. 8.2.3 auf S. 112).
- Parameter, welche die Aktionen für gefährliche E-Mail-Objekte definieren (s. Pkt. 8.2.6 auf S. 116).

In diesem Abschnitt des Handbuchs werden alle oben genannten Parameter ausführlich beschrieben.

8.2.1. Auswahl der zu schützenden Richtung der Nachrichten

Mail-Anti-Virus erlaubt Ihnen, auszuwählen, in welcher Richtung die E-Mail-Nachrichten auf gefährliche Objekte untersucht werden.

Standardmäßig schützt die Komponente Ihre Post entsprechend den Parametern der Schutzstufe **Empfohlen**, d.h. die ein- und ausgehende Post wird untersucht. Zu Beginn der Arbeit mit dem Programm ist es empfehlenswert, die ausgehende Post zu untersuchen, weil die Möglichkeit besteht, dass sich Mailwürmer auf Ihrem Computer befinden, die E-Mails als Kanal verwenden, um sich weiterzuverbreiten. Dadurch wird erlaubt, Probleme zu verhindern, die mit dem unkontrollierten Versenden infizierter E-Mail-Nachrichten von Ihrem Computer verbunden sind.

Wenn Sie sicher sind, dass die von Ihnen gesendeten Briefe keine gefährlichen Objekte enthalten, können Sie die Untersuchung der ausgehenden Post folgendermaßen deaktivieren:

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie im Abschnitt **Schutz** die Komponente **Mail-Anti-Virus**.
2. Klicken Sie im Block **Sicherheitsstufe** (s. Abb. 25) auf die Schaltfläche **Einstellungen**.
3. Wählen Sie im folgenden Fenster (s. Abb. 26) im Block **Schutzbereich** die Variante **Nur eingehende E-Mails**

Neben der Auswahl der Richtung können Sie festlegen, ob an E-Mails angehängte Archive kontrolliert werden sollen. Außerdem kann die maximale Untersuchungszeit für ein E-Mail-Objekt angepasst werden. Diese Parameter befinden sich im Block **Optimierung**.

Wenn Ihr Computer nicht durch die Mittel eines lokalen Netzwerks geschützt ist und die Internetverbindung ohne Proxyserver oder Firewall erfolgt, wird empfohlen, die Untersuchung angehängter Archive nicht zu deaktivieren und keine Zeitbeschränkung für die Objektuntersuchung festzulegen.

Wenn Sie in einer geschützten Umgebung arbeiten, kann eine Zeitbeschränkung für die Objektuntersuchung festgelegt werden, um das Tempo der E-Mail-Untersuchung zu steigern.

Abbildung 26. Einstellungen für den Schutz des Maildatenstroms

Im Block **Filter für angehängte Dateien** können Sie die Filterbedingungen für an E-Mail-Nachrichten angehängte Objekte festlegen:

- **Filter nicht anwenden** – keine zusätzliche Filterung für Attachments verwenden.
- **Anhänge der genannten Typen umbenennen** – angehängte Dateien eines bestimmten Formats ausfiltern und das letzte Zeichen des Dateinamens durch das Zeichen "Unterstrich" ersetzen. Das Fenster zur Auswahl der Dateitypen wird mit der Schaltfläche **Dateitypen** geöffnet.
- **Anhänge der genannten Typen löschen** – angehängte Dateien eines bestimmten Formats ausfiltern und löschen. Das Fenster zur Auswahl der Dateitypen wird mit der Schaltfläche **Dateitypen** geöffnet.

> **Hinweis**
>
> Details über die Typen der angehängten Dateien, die der Filterung unterzogen werden, finden Sie in Anhang A.1 auf S. 256.

Die Verwendung des Filters bietet Ihrem Computer zusätzliche Sicherheit, da sich Schadprogramme über E-Mails meist in Form angehängter Dateien verbreiten. Das Umbenennen oder Löschen von Attachments eines bestimmten Typs erlaubt es, Ihren Computer beispielsweise davor zu schützen, dass eine angehängte Datei beim Empfang einer Nachricht automatisch geöffnet wird.

8.2.2. Anpassen der E-Mail-Untersuchung in Microsoft Office Outlook

Wenn Sie Microsoft Office Outlook als Mailprogramm verwenden, können Sie die Virenuntersuchung Ihrer Post zusätzlich anpassen.

Bei der Installation von Kaspersky Anti-Virus wird ein spezielles Erweiterungsmodul in Microsoft Office Outlook integriert. Es erlaubt Ihnen, schnell zu den Einstellungen von Mail-Anti-Virus zu wechseln und festzulegen, zu welchem Zeitpunkt eine E-Mail-Nachricht auf das Vorhandensein gefährlicher Objekte untersucht werden soll.

Das Erweiterungsmodul besitzt die Form einer speziellen Registerkarte mit dem Namen **Mail-Anti-Virus**, die sich im Menü **Extras** → **Optionen** befindet (s. Abb. 27).

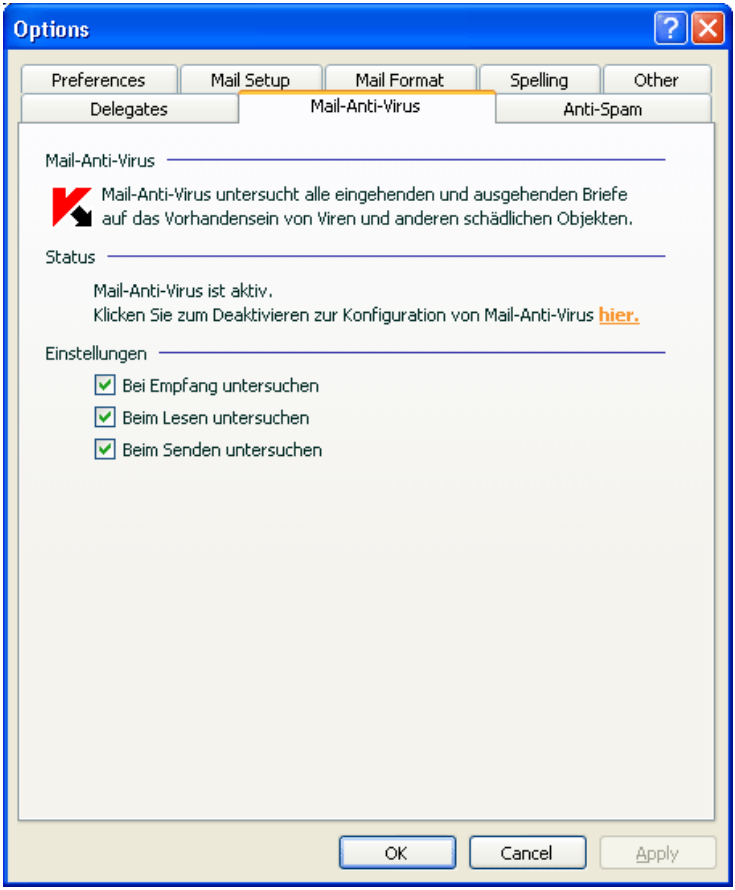


Abbildung 27. Detaillierte Konfiguration des E-Mail-Schutzes in Microsoft Office Outlook

Wählen Sie den Modus für die E-Mail-Untersuchung:

- **Bei Empfang untersuchen** – Jede E-Mail-Nachricht wird im Moment ihres Eintreffens in Ihrer Mailbox untersucht.
- **Beim Lesen untersuchen** – E-Mails werden dann untersucht, wenn sie zum Lesen geöffnet werden.
- **Beim Senden untersuchen** – Jede E-Mail-Nachricht, die Sie senden möchten, wird im Moment des Sendens auf Viren untersucht.

Achtung!

Wenn Sie zur Verbindung von Microsoft Office Outlook mit dem Mailserver das Protokoll IMAP verwenden, wird empfohlen, den Modus **Bei Empfang untersuchen** nicht zu benutzen. Wenn dieser Modus aktiviert wird, werden die auf dem Server eintreffenden E-Mails zwangsläufig auf den lokalen Computer kopiert. Dadurch geht der Hauptvorteil des IMAP-Protokolls verloren, der in der Einsparung von Netzwerkverkehr und in der Verwaltung unerwünschter Briefe auf dem Server ohne Kopieren auf den Benutzercomputer besteht.

Die Aktion, die mit gefährlichen E-Mail-Objekten erfolgt, wird in den Einstellungen für Mail-Anti-Virus festgelegt, zu denen Sie über den Link hier wechseln können.

8.2.3. Anpassen der E-Mail-Untersuchung in The Bat!

Die Aktionen für infizierte E-Mail-Objekte werden im Mailprogramm The Bat! durch Mittel des Programms festgelegt.

Achtung!

Die Parameter von Mail-Anti-Virus, die festlegen, ob ein- und ausgehende Post untersucht werden oder nicht, und die Aktionen für gefährliche E-Mail-Objekte und Ausnahmen bestimmen, werden ignoriert. Das Programm The Bat! berücksichtigt lediglich folgende Parameter: Untersuchung angehängter Archive und Zeitbeschränkung für die Untersuchung eines E-Mail-Objekts (s. Pkt. 8.2.1 auf S. 108).

Um in The Bat! die Regeln für die Einstellungen für den Mail-Schutz anzupassen,

1. Wählen Sie im Menü **Optionen** des Mailprogramms den Punkt **Benutzereinstellungen**.
2. Wählen Sie in der Konfigurationsstruktur den Punkt **Anti-Virus-Plugins**.

Die hier angezeigten Parameter für den E-Mail-Schutz (s. Abb. 28) gelten für alle auf dem Computer installierten Antiviren-Module, welche die Arbeit mit The Bat! unterstützen.

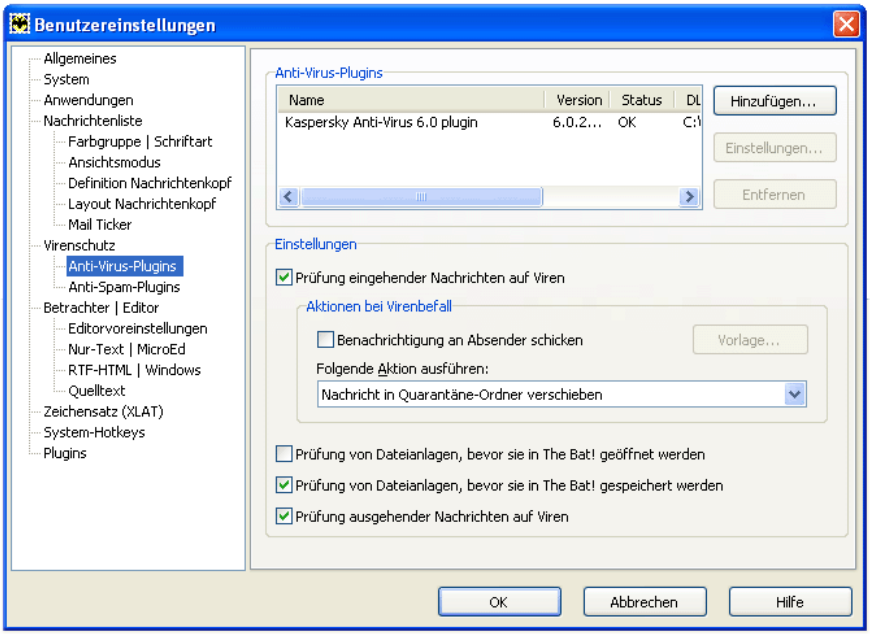


Abbildung 28. Untersuchungseinstellungen in The Bat!

Folgende Einstellungen sind erforderlich:

- Welche Richtung des E-Mail-Verkehrs (eingehende, ausgehende) soll der Virenprüfung unterzogen werden.
- In welchem Moment soll die Virenuntersuchung der E-Mail-Objekte erfolgen (beim Öffnen eines Briefs, vor dem Speichern auf der Festplatte).
- Aktionen, die das Mailprogramm beim Fund gefährlicher Objekte in E-Mail-Nachrichten ausführen soll. Es stehen beispielsweise zur Auswahl:

  Reparaturversuch infizierter Teile – Es wird versucht, das infizierte E-Mail-Objekt zu desinfizieren. Wenn die Desinfektion unmöglich ist, verbleibt das Objekt im Brief. Kaspersky Anti-Virus benachrichtigt Sie darüber, dass ein Objekt der E-Mail-Nachricht infiziert ist. Doch selbst wenn Sie in der Meldung von Mail-Anti-Virus die Aktion **Löschen** wählen, verbleibt das Objekt in der E-Mail-Nachricht, weil die in The Bat! gewählte Aktion höhere Priorität besitzt, als die Aktion von Mail-Anti-Virus.

  Infizierte Teile löschen – Ein gefährliches E-Mail-Objekt wird gelöscht, wenn es infiziert ist oder als verdächtig gilt.

Standardmäßig verschiebt das Programm The Bat! alle infizierten E-Mail-Objekte ohne Desinfektion in den Ordner Quarantäne.

Achtung!

E-Mail-Nachrichten, die gefährliche Objekte enthalten, werden von dem Programm The Bat! nicht durch eine spezielle Kopfzeile gekennzeichnet.

8.2.4. Verwendung von heuristischen Analysemethoden

Heuristische Analysemethoden werden bei der Arbeit bestimmter Echtzeitschutz-Komponenten und bei Aufgaben zur Virensuche verwendet (Details s. Pkt. 7.2.4 auf S. 98).

Auf der Registerkarte **Heuristische Analyse** (s. Abb. 23) können Sie die Verwendung von heuristischen Methoden zur Suche neuer Bedrohungen bei der Arbeit der Komponente Mail-Anti-Virus aktivieren/deaktivieren. Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie im Abschnitt **Schutz** die Komponente **Mail-Anti-Virus**.
2. Klicken Sie im Block **Sicherheitsstufe** (s. Abb. 25) auf die Schaltfläche **Einstellungen**.
3. Wählen Sie im folgenden Fenster die Registerkarte **Heuristische Analyse** (s. Abb. 29).

Um die heuristischen Methoden zu verwenden, aktivieren Sie das Kontrollkästchen ☑ **Heuristische Analyse verwenden**. Sie können zusätzlich die Genauigkeitsstufe der Untersuchung anpassen. Bewegen Sie dazu den Schieberegler auf die gewünschte Position: **Oberflächlich**, **Mittel** oder **Detailliert**.

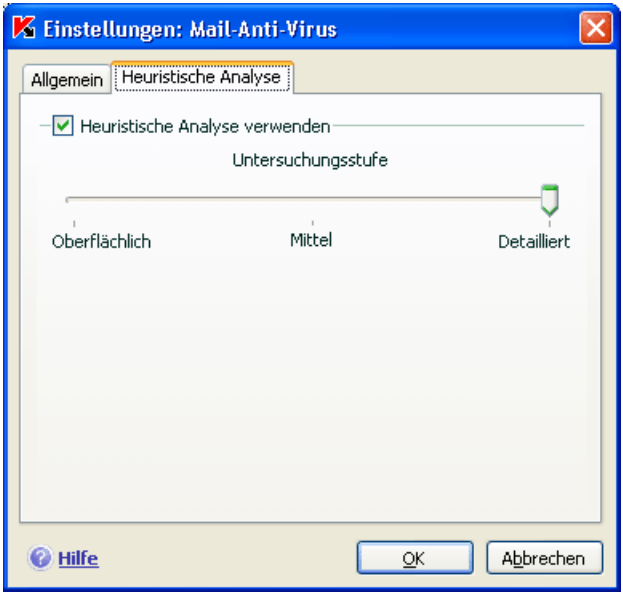


Abbildung 29. Verwendung von heuristischen Analysemethoden

8.2.5. Wiederherstellen der Standardparameter für den Mail-Schutz

Während Sie die Arbeit von Mail-Anti-Virus anpassen, können Sie jederzeit zu den empfohlenen Einstellungen zurückkehren. Diese gelten als optimal, werden von den Kaspersky-Lab-Spezialisten empfohlen und sind in der Sicherheitsstufe **Empfohlen** zusammengefasst.

Um die standardmäßigen Parameter für den Mail-Schutz wiederherzustellen,

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie im Abschnitt **Schutz** die Komponente **Mail-Anti-Virus**.
2. Klicken Sie im Block **Sicherheitsstufe** (s. Abb. 25) auf die Schaltfläche **Grundeinstellung**.

8.2.6. Auswahl der Aktion für ein gefährliches E-Mail-Objekt

Wenn sich durch die Virenuntersuchung einer E-Mail-Nachricht herausstellt, dass ein Brief oder ein E-Mail-Objekt (Briefkörper, Anhang) infiziert oder verdächtig ist, hängen die weiteren Operationen von Mail-Anti-Virus vom Status des Objekts und der ausgewählten Aktion ab.

Ein E-Mail-Objekt kann aufgrund der Untersuchung einen der folgenden Status erhalten:

- Status eines der schädlichen Programme (beispielsweise *Virus*, *trojanisches Programm*, Details s. Pkt. 1.3 auf S. 12).
- *möglicherweise infiziert*, wenn sich aufgrund der Untersuchung nicht eindeutig feststellen lässt, ob das Objekt infiziert ist oder nicht. Das bedeutet, dass in der Datei die Codefolge eines unbekannten Virus oder der modifizierte Code eines bekannten Virus gefunden wurde.

Standardmäßig zeigt Mail-Anti-Virus beim Fund eines gefährlichen oder möglicherweise infizierten Objekts auf dem Bildschirm eine Warnung an und bietet mehrere Aktionen für das Objekt zur Auswahl an.

Um die Aktion für ein Objekt zu ändern,

öffnen Sie das Konfigurationsfenster des Programms und wählen Sie im Abschnitt **Schutz** die Komponente **Mail-Anti-Virus**. Alle verfügbaren Aktionen für gefährliche Objekte werden im Block **Aktion** genannt (s. Abb. 30).

Abbildung 30. Auswahl der Aktion für ein gefährliches E-Mail-Objekt

Betrachten wir die möglichen Varianten zur Bearbeitung gefährlicher E-Mail-Objekte genauer:

Gewählte Aktion	Was geschieht beim Fund eines gefährlichen Objekts?
Aktion erfragen	Mail-Anti-Virus zeigt eine Warnmeldung auf dem Bildschirm an, die darüber informiert, von was für einem schädlichen Objekt die E-Mail infiziert (möglicherweise infiziert) ist, und bietet Aktionen zur Auswahl an.
Zugriff verweigern	Mail-Anti-Virus blockiert den Zugriff auf das Objekt. Informationen darüber werden im Bericht aufgezeichnet (s. Pkt. 15.3 auf S. 195). Später kann versucht werden, das Objekt zu desinfizieren.
Zugriff verweigern **Desinfizieren**	Mail-Anti-Virus blockiert den Zugriff auf das Objekt und versucht, es zu desinfizieren. Wenn das Objekt desinfiziert werden konnte, wird es zur Arbeit freigegeben. Wenn der Desinfektionsversuch erfolglos war, wird das Objekt in die Quarantäne verschoben. Informationen darüber werden im Bericht aufgezeichnet. Später kann versucht werden, das Objekt zu desinfizieren.
Zugriff verweigern **Desinfizieren** **Löschen, wenn Desinfektion nicht möglich**[2]	Mail-Anti-Virus blockiert den Zugriff auf das Objekt und versucht, es zu desinfizieren. Wenn das Objekt desinfiziert werden konnte, wird es zur Arbeit freigegeben. Wenn der Desinfektionsversuch erfolglos war, wird es gelöscht. Dabei wird eine Kopie des Objekts im Backup gespeichert. Ein Objekt mit dem Status *möglicherweise infiziert* wird in die Quarantäne verschoben.

[2] Wenn The Bat! als Mailprogramm verwendet wird, werden bei dieser Aktion gefährliche E-Mail-Objekte entweder desinfiziert oder gelöscht (abhängig davon, welche Aktion in The Bat! gewählt wurde).

Gewählte Aktion	Was geschieht beim Fund eines gefährlichen Objekts?
Zugriff verweigern **Löschen**	Mail-Anti-Virus blockiert den Zugriff auf das infizierte oder möglicherweise infizierte Objekt und löscht es.

Bevor ein Desinfektionsversuch erfolgt oder das Objekt gelöscht wird, legt Kaspersky Anti-Virus eine Sicherungskopie des Objekts an und speichert diese im Backup (s. Pkt. 15.2 auf S. 193). Dadurch wird erlaubt, das Objekt bei Bedarf wiederherzustellen oder später zu desinfizieren.

KAPITEL 9. WEB-SCHUTZ

Bei der Arbeit im Internet besteht für die Informationen, die auf Ihrem Computer gespeichert sind, ständig das Risiko einer Infektion durch gefährliche Programme. Sie können in den Computer eindringen, während Sie im Internet bestimmte Seiten besuchen.

Um die Sicherheit Ihrer Arbeit im Internet zu garantieren, enthält Kaspersky Anti-Virus eine spezielle Komponente: *Web-Anti-Virus*. Er schützt Informationen, die über das HTTP-Protokoll auf Ihren Computer gelangen, und verhindert den Start gefährlicher Skripts auf Ihrem Computer.

Achtung!

Der Web-Schutz sieht die Kontrolle des HTTP-Datenverkehrs vor, der nur über die Ports, die in der Liste zu kontrollierenden Ports (s. Pkt. 15.4 auf S. 204) angegeben sind, vor. Eine Liste der Ports, die am häufigsten zur Übertragung von E-Mails und HTTP-Datenverkehr benutzt werden, ist im Lieferumfang des Programms enthalten. Wenn Sie Ports verwenden, die nicht zu dieser Liste gehören, sollten diese der Liste hinzugefügt werden, um den Schutz des über sie abgewickelten Datenverkehrs zu gewährleisten.

Wenn Sie in einer ungeschützten Umgebung arbeiten, ist es empfehlenswert, Web-Anti-Virus zum Schutz Ihrer Arbeit im Internet zu verwenden. Wenn Ihr Computer in einem Netzwerk arbeitet, das durch eine Firewall oder durch Filter für den HTTP-Verkehr geschützt ist, gewährleistet Web-Anti-Virus zusätzlichen Schutz bei der Arbeit im Internet.

Als Indikator für die Arbeit der Komponente dient das Symbol von Kaspersky Anti-Virus im Infobereich der Taskleiste von Microsoft Windows, das jedes Mal bei der Untersuchung von Skripts folgendes Aussehen annimmt: .

Im Folgenden wird das Funktionsschema der Komponente näher beschrieben.

Web-Anti-Virus besteht aus zwei Modulen mit folgenden Funktionen:

- *Schutz des HTTP-Verkehrs* – Untersuchung aller Objekte, die über HTTP-Protokoll auf dem Computer eintreffen.
- *Skriptuntersuchung* – Untersuchung aller Skripts, die in Microsoft Internet Explorer bearbeitet werden, sowie aller WSH-Skripts (JavaScript, Visual Basic Script u.a.), die bei der Arbeit des Benutzers auf dem Computer und im Internet gestartet werden sollen.

  Für das Programm Microsoft Internet Explorer ist ein spezielles Erweiterungsmodul vorgesehen, das bei der Installation von Kaspersky Anti-

Virus in das Programm integriert wird. Es erlaubt die Ansicht einer Statistik über die von Web-Anti-Virus gesperrten gefährlichen Skripts. Über sein Vorhandensein informiert die Schaltfläche in der Symbolleiste des Browsers. Durch Klick auf diese Schaltfläche wird eine Infoleiste mit einer Statistik für Web-Anti-Virus geöffnet, welche die Anzahl der untersuchten und blockierten Skripts anzeigt.

Der Schutz des HTTP-Verkehrs erfolgt nach folgendem Algorithmus:

1. Jede Webseite oder Datei, auf die der Benutzer oder ein bestimmtes Programm über das Protokoll HTTP zugreift, wird von Web-Anti-Virus abgefangen und auf schädlichen Code analysiert. Die Suche nach schädlichen Objekten erfolgt auf Basis der *Datenbanken*, die bei der Arbeit von Kaspersky Anti-Virus verwendet werden, sowie mit Hilfe eines heuristischen Algorithmus. Die Datenbanken enthalten eine Beschreibung aller momentan bekannten schädlichen Programme und Methoden zu deren Desinfektion. Der heuristische Algorithmus erlaubt es, neue Viren zu erkennen, die noch nicht in den Datenbanken beschrieben sind.
2. Aufgrund der Virenuntersuchung bestehen folgende Varianten für das weitere Vorgehen:
   - Wenn eine Webseite oder ein Objekt, auf das der Benutzer zugreift, schädlichen Code enthält, wird der Zugriff blockiert. Dabei erscheint auf dem Bildschirm eine Meldung darüber, dass das angeforderte Objekt oder die Seite infiziert ist.
   - Wenn eine Datei oder eine Webseite keinen schädlichen Code enthält, erhält der Benutzer sofort Zugriff darauf

Die Untersuchung von Skripts wird nach folgendem Algorithmus ausgeführt:

1. Jedes auf einer Webseite auszuführende Skript wird von Web-Anti-Virus abgefangen und auf schädlichen Code analysiert.
2. Wenn das Skript schädlichen Code enthält, sperrt Web-Anti-Virus es und benachrichtigt den Benutzer durch eine spezielle Popup-Meldung.
3. Wenn im Skript kein schädlicher Code gefunden wird, wird es ausgeführt.

Achtung!

Damit http-Datenverkehr und Skripts von abgefangen und auf Viren untersucht werden, muss Web-Anti-Virus gestartet werden, bevor eine Verbindung mit einer Ressource hergestellt wird. Andernfalls wird der Datenverkehr nicht untersucht.

9.1. Auswahl der Web-Sicherheitsstufe

Kaspersky Anti-Virus bietet die Sicherheit Ihrer Arbeit im Internet auf einer der folgenden Stufen (s. Abb. 31):

Maximaler Schutz – Auf dieser Stufe erfolgt die Kontrolle von Skripts und Objekten, die über HTTP-Protokoll eintreffen, mit maximaler Ausführlichkeit. Das Programm untersucht ausführlich alle Objekte und verwendet dabei die vollständige Auswahl der Bedrohungssignaturen. Die Verwendung dieser Stufe wird in einer aggressiven Umgebung empfohlen, wenn keine anderen Mittel zum Schutz des HTTP-Verkehrs benutzt werden.

Empfohlen. Die Parameter dieser Stufe entsprechen den von Kaspersky Lab empfohlenen Einstellungen. Sie umfassen die Untersuchung der gleichen Objekte wie auf der Stufe **Maximaler Schutz**. Allerdings ist die Zeit für die Zwischenspeicherung eines Dateifragments begrenzt, was erlaubt, die Untersuchung und Weiterleitung des Objekts an den Benutzer zu beschleunigen.

Maximales Tempo – Diese Sicherheitsstufe erlaubt Ihnen, bequem mit Anwendungen, die den Arbeitsspeicher stark beanspruchen, zu arbeiten, weil die Auswahl der untersuchten Objekte auf dieser Stufe aufgrund der Verwendung einer beschränkten Auswahl von Programm-Datenbanken eingeschränkt wird. Es wird empfohlen, diese Sicherheitsstufe zu wählen, wenn auf dem Computer zusätzliche Mittel zum Web-Schutz installiert sind.

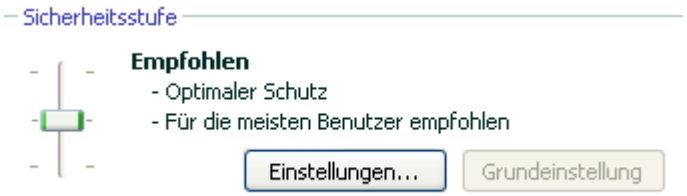


Abbildung 31. Auswahl der Sicherheitsstufe für Web-Anti-Virus

Der Web-Schutz erfolgt standardmäßig auf der **Empfohlenen** Stufe.

Sie können die Schutzstufe für Ihre Arbeit im Internet erhöhen oder senken, indem Sie die entsprechende Stufe wählen oder die Einstellungen der aktuellen Stufe ändern.

Um die Sicherheitsstufe zu ändern,

verschieben Sie den Zeiger auf der Skala. Durch das Anpassen der Schutzstufe wird das Verhältnis zwischen der Ausführungsgeschwindigkeit der Untersuchung und der Anzahl der zu untersuchenden Objekte bestimmt: Je weniger Objekte der Analyse auf schädlichen Code unterzogen werden, desto höher ist die Untersuchungsgeschwindigkeit.

Wenn eine der vordefinierten Stufen nicht vollständig Ihren Anforderungen entspricht, können Sie die Schutzparameter zusätzlich anpassen. Wählen Sie dazu die Stufe, die Ihren Anforderungen am nächsten kommt, als Ausgangsstufe und ändern Sie ihre Parameter entsprechend. In diesem Fall ändert sich der Name der Stufe in **Benutzerdefiniert**. Betrachten wir ein Beispiel dafür, wann eine Änderung der vordefinierten Sicherheitsstufen nützlich sein kann.

Beispiel:

Ihr Computer wird über ein Modem mit dem Internet verbunden. Er ist nicht Teil eines lokalen Firmennetzwerks und ein Virenschutz des eingehenden HTTP-Verkehrs ist nicht vorhanden.

Bedingt durch die Besonderheiten Ihrer Arbeit laden Sie häufig große Dateien aus dem Internet herunter. In der Regel benötigt die Untersuchung solcher Dateien relativ viel Zeit.

Wie können Sie Ihren Computer optimal vor einer Infektion über den HTTP-Verkehr oder Skripts schützen?

Empfehlung zur Auswahl der Stufe:

Die Analyse der Situation lässt den Schluss zu, dass Ihr Computer in einer aggressiven Umgebung arbeitet und die Infektionsgefahr durch ein Schadprogramm über den HTTP-Verkehr sehr groß ist (Fehlen eines zentralen Web-Schutzes und Verbindungsmethode zum Internet).

Es wird empfohlen, von der vordefinierten Sicherheitsstufe **Maximaler Schutz** auszugehen und diese folgendermaßen anzupassen: Die Zeitbegrenzung für die Zwischenspeicherung von Dateifragmenten bei der Untersuchung wird angepasst.

Um die Einstellungen einer vordefinierten Sicherheitsstufe anzupassen,

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie im Abschnitt **Schutz** die Komponente **Web-Anti-Virus**.
2. Klicken Sie im Block **Sicherheitsstufe** (s. Abb. 31) auf die Schaltfläche **Einstellungen**.
3. Passen Sie im folgenden Fenster die Parameter für den Web-Schutz an und klicken Sie dann auf **OK**.

9.2. Konfiguration des Web-Schutzes

Der Web-Schutz garantiert die Untersuchung aller Objekte, die mit dem HTTP-Protokoll auf Ihren Computer heruntergeladen werden, und bietet die Kontrolle über alle WSH-Skripts (JavaScript, Visual Basic Script u.a.), die gestartet werden sollen.

Sie können folgende Parameter für Web-Anti-Virus anpassen, welche der beschleunigten Arbeit der Komponente dienen:

- Allgemeine Untersuchungsparameter festlegen (s. Pkt. **Error! Reference source not found.** auf S. **Error! Bookmark not defined.**).
- Sie können eine Liste der Adressen anlegen, deren Inhalt Sie vertrauen (s. Pkt. 9.2.2 auf S. 125).
- Sie können die Verwendung der heuristischen Analysemethoden aktivieren/deaktivieren (s. Pkt. 9.2.3 auf S. 126).

Außerdem können Sie die Aktion für gefährliche Objekte im HTTP-Verkehr wählen, die von Web-Anti-Virus damit ausgeführt werden soll.

In diesem Abschnitt des Handbuchs werden alle oben genannten Parameter ausführlich beschrieben.

9.2.1. Allgemeine Untersuchungsparameter

Um die Malware-Erkennung zu optimieren, verwendet Web-Anti-Virus die Zwischenspeicherung von Fragmenten der Objekte, die aus dem Internet empfangen werden. Bei der Verwendung dieser Technologie erfolgt die Untersuchung eines Objekts erst, nachdem Web-Anti-Virus es vollständig empfangen hat. Das Objekt wird dann der Virenanalyse unterzogen und in Abhängigkeit von den Untersuchungsergebnissen dem Benutzer zur Arbeit übergeben oder blockiert.

Allerdings erhöht sich durch die Verwendung der Zwischenspeicherung die Zeit für die Objektuntersuchung und für dessen Freigabe an den Benutzer. Außerdem können beim Kopieren und bei der Bearbeitung großer Objekte Probleme auftreten, die mit einer Zeitüberschreitung bei der Verbindung mit dem HTTP-Client zusammenhängen.

Um das Problem zu lösen, wird empfohlen, die Zeit für die Zwischenspeicherung von Fragmenten eines aus dem Internet empfangenden Objekts zu beschränken. Bei einer Überschreitung des Zeitlimits wird jeder heruntergeladene Teil der Datei ungeprüft dem Benutzer übergeben und erst nach Abschluss des Downloads wird das Objekt vollständig untersucht. Dadurch lässt sich die Dauer für die Übertragung des Objekts an den Benutzer verringern und das Problem einer

Verbindungsstörung lösen, ohne das Sicherheitsniveau bei der Arbeit im Internet einzuschränken.

In der Grundeinstellung beträgt der Grenzwert für die Zwischenspeicherung von Dateifragmenten 1 Sekunde. Ein höherer Wert oder die Aufhebung der Zeitbeschränkung für die Zwischenspeicherung steigert das Niveau der Antiviren-Untersuchung, kann aber auch zu verzögerten Zugriff auf das Objekt führen.

Um eine Zeitbeschränkung für die Zwischenspeicherung von Fragmenten festzulegen oder die Beschränkung aufzuheben:

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie im Abschnitt **Schutz** die Komponente **Web-Anti-Virus**.
2. Klicken Sie im Block **Sicherheitsstufe** (s. Abb. 31) auf die Schaltfläche **Einstellungen**.
3. Wählen Sie im folgenden Fenster (s. Abb. 32) im Block **Untersuchungsparameter** den gewünschten Wert.

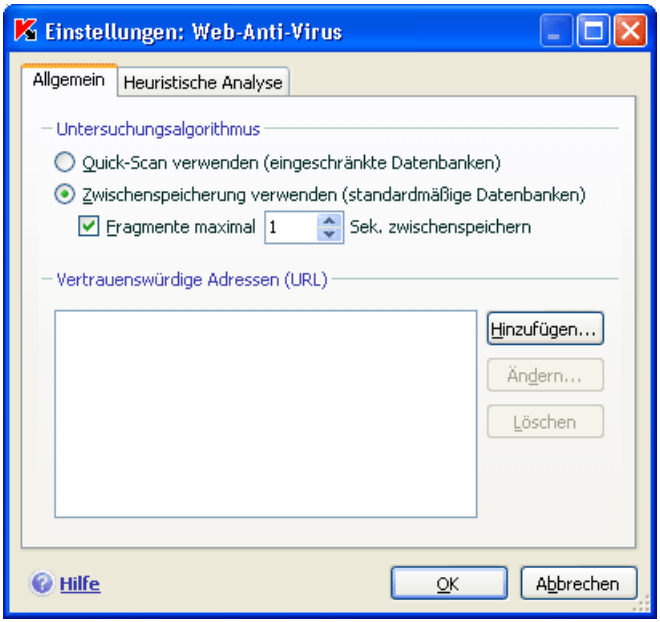


Abbildung 32. Einstellungen der Web-Schutzstufe

9.2.2. Erstellen einer Liste der vertrauenswürdigen Adressen

Ihnen wird die Möglichkeit geboten, eine Liste der vertrauenswürdigen Adressen anzulegen, deren Inhalt Sie vorbehaltlos vertrauen. Web-Anti-Virus wird die Informationen von diesen Adressen nicht auf gefährliche Objekte hin analysieren. Diese Option kann benutzt werden, wenn Web-Anti-Virus das Laden einer bestimmten Datei verhindert, indem er den Downloadversuch blockiert.

Um eine Liste mit vertrauenswürdigen Adressen anzulegen,

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie im Abschnitt **Schutz** die Komponente **Web-Anti-Virus**.
2. Klicken Sie im Block **Sicherheitsstufe** (s. Abb. 31) auf die Schaltfläche **Einstellungen**.
3. Erstellen Sie im folgenden Fenster (s. Abb. 32) im Block **Vertrauenswürdige Adressen (URL)** die Liste der vertrauenswürdigen Adressen. Rechts der Liste sind entsprechende Schaltflächen vorhanden.

Bei der Angabe einer vertrauenswürdigen Adresse können Sie Masken benutzen, die folgende Sonderzeichen enthalten:

***** – beliebige Zeichenfolge.
Beispiel: Wird die Maske ***abc*** angegeben, dann wird eine beliebige URL-Adresse, in der die Zeichenfolge **abc** enthalten ist, nicht untersucht. Beispiel: www.virus.com/download_virus/page_0-9abcdef.html.

? – ein beliebiges Zeichen.
Beispiel: Bei Angabe der Maske **Patch_123?.com** wird eine URL-Adresse nicht untersucht, die diese Zeichenfolge und ein beliebiges Zeichen enthält, das auf die 3 folgt, beispielsweise **Patch_1234.com**. Die Adresse **patch_12345.com** wird dagegen untersucht.

Wenn die Zeichen ***** und **?** Bestandteil einer realen URL-Adresse sind, die der Liste hinzugefügt werden soll, dann muss bei der Angabe das Zeichen **** benutzt werden, damit eines der Zeichen *****, **?**, **** nicht als Platzhalter interpretiert wird.

Beispiel: Folgende URL-Adresse soll als vertrauenswürdige Adresse festgelegt werden: www.virus.com/download_virus/virus.dll?virus_name=

Damit Kaspersky Anti-Virus das Zeichen **?** nicht als Zeichen für eine Ausnahme interpretiert, muss dem **?** das Zeichen **** vorangestellt werden. In diesem Fall muss die URL-Adresse also in folgender Form zur Liste der Ausnahmen hinzugefügt werden: www.virus.com/download_virus/virus.dll\?virus_name=

9.2.3. Verwendung von heuristischen Analysemethoden

Heuristische Analysemethoden werden bei der Arbeit bestimmter Echtzeitschutz-Komponenten und bei Aufgaben zur Virensuche verwendet (Details s. Pkt. 7.2.4 auf S. 98).

Auf der Registerkarte **Heuristische Analyse** können Sie die Verwendung von heuristischen Methoden zur Suche neuer Bedrohungen bei der Arbeit der Komponente Web-Anti-Virus aktivieren/deaktivieren. Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie im Abschnitt **Schutz** die Komponente **Web-Anti-Virus**.
2. Klicken Sie im Block **Sicherheitsstufe** auf die Schaltfläche **Einstellungen**.
3. Wählen Sie im folgenden Fenster die Registerkarte **Heuristische Analyse** (s. Abb. 33).

Um die heuristischen Methoden zu verwenden, aktivieren Sie das Kontrollkästchen ☑ **Heuristische Analyse verwenden**. Sie können zusätzlich die Genauigkeitsstufe der Untersuchung anpassen. Bewegen Sie dazu den Schieberegler auf die gewünschte Position: **Oberflächlich**, **Mittel** oder **Detailliert**.

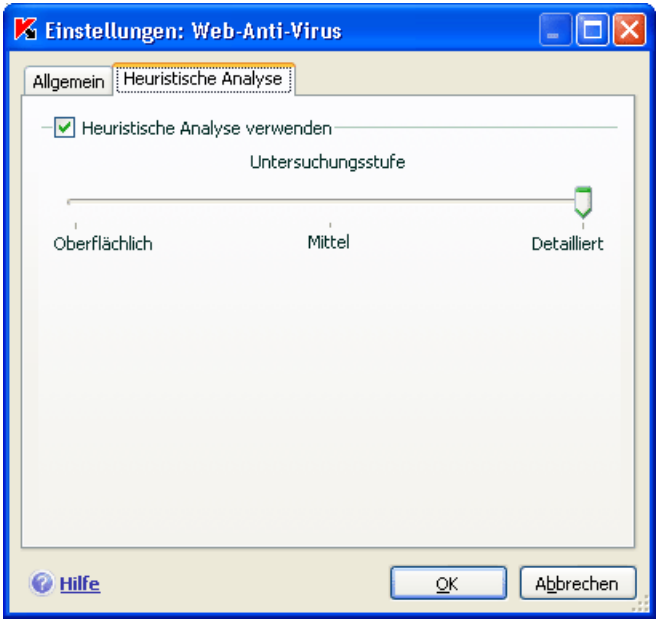


Abbildung 33. Verwendung von heuristischen Analysemethoden

9.2.4. Wiederherstellen der Standardparameter für den Web-Schutz

Während Sie die Arbeit von Web-Anti-Virus anpassen, können Sie jederzeit zu den empfohlenen Einstellungen zurückkehren. Diese gelten als optimal, werden von den Kaspersky-Lab-Spezialisten empfohlen und sind in der Sicherheitsstufe **Empfohlen** zusammengefasst.

Um die standardmäßigen Parameter für Web-Anti-Virus wiederherzustellen,

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie im Abschnitt **Schutz** die Komponente **Web-Anti-Virus**.
2. Klicken Sie im Block **Sicherheitsstufe** (s. Abb. 31)) auf die Schaltfläche **Grundeinstellung**.

9.2.5. Auswahl der Aktion für ein gefährliches Objekt

Wenn sich durch die Analyse eines Objekts des HTTP-Verkehrs herausstellt, dass das Objekt schädlichen Code enthält, sind die weiteren Operationen von Web-Anti-Virus von der Aktion abhängig, die Sie festgelegt haben.

Um die Reaktion von Web-Anti-Virus beim Fund eines gefährlichen Objekts zu bestimmen:

öffnen Sie das Konfigurationsfenster des Programms und wählen Sie im Abschnitt **Schutz** die Komponente **Web-Anti-Virus**. Alle verfügbaren Aktionen für gefährliche Objekte sind im Block **Aktion** angegeben (s. Abb. 34).

Standardmäßig zeigt Web-Anti-Virus beim Fund eines gefährlichen Objekts im HTTP-Verkehr auf dem Bildschirm eine Warnung an und bietet mehrere Aktionen für das Objekt zur Auswahl an.

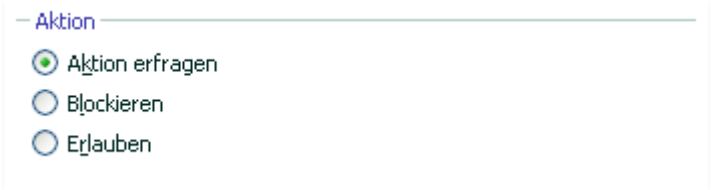


Abbildung 34. Auswahl der Aktion für ein gefährliches Skript

Betrachten wir die möglichen Varianten zur Bearbeitung gefährlicher Objekte des HTTP-Verkehrs genauer.

Gewählte Aktion	Was geschieht beim Fund eines gefährlichen Objekts im HTTP-Verkehr?
Aktion erfragen	Web-Anti-Virus zeigt eine Warnmeldung auf dem Bildschirm an, die darüber informiert, von welchem schädlichen Code das Objekt infiziert ist, und bietet Aktionen zur Auswahl an.
Blockieren	Web-Anti-Virus sperrt den Zugriff auf das Objekt und zeigt eine Meldung über das Blockieren auf dem Bildschirm an. Informationen darüber werden im Bericht aufgezeichnet (s. Pkt. 15.3 auf S. 195).
Erlauben	Web-Anti-Virus erlaubt den Zugriff auf das Objekt.

Gewählte Aktion	**Was geschieht beim Fund eines gefährlichen Objekts im HTTP-Verkehr?**
	Informationen darüber werden im Bericht aufgezeichnet.

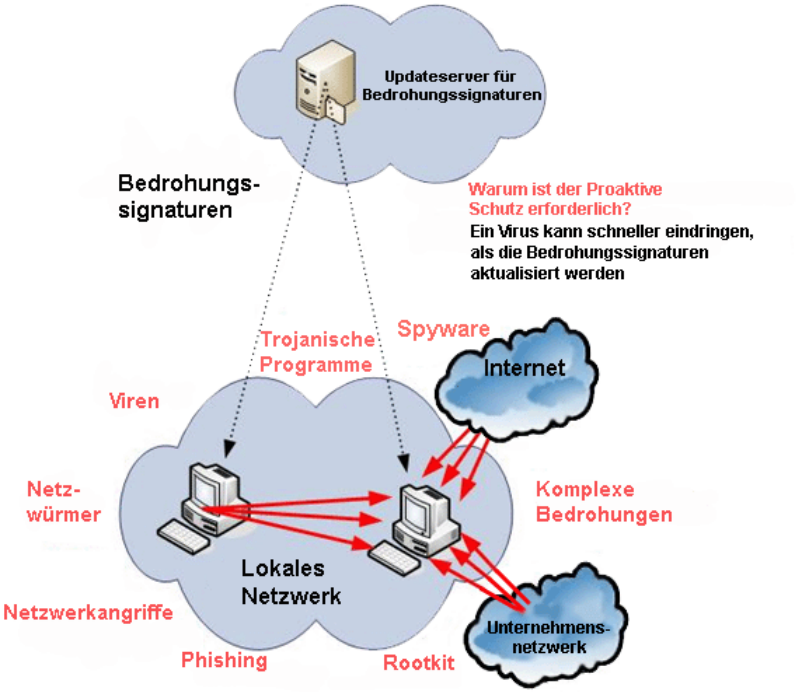
Web-Anti-Virus sperrt die Ausführung gefährlicher Skripts und zeigt auf dem Bildschirm eine Popup-Meldung an, die den Benutzer über die ausgeführte Aktion informiert. Die Aktion für ein gefährliches Skript kann nicht vom Benutzer geändert werden. Es besteht höchstens die Möglichkeit, die Arbeit des Moduls zur Skriptuntersuchung zu deaktivieren.

KAPITEL 10. PROAKTIVER SCHUTZ FÜR IHREN COMPUTER

Achtung!

Für Computer mit dem Betriebssystem Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista oder Microsoft Windows Vista x64 ist in dieser Version der Anwendung die Komponente **Integritätskontrolle für Anwendungen** nicht vorhanden.

Kaspersky Anti-Virus schützt nicht nur vor bekannten, sondern auch vor neuen Bedrohungen, über die noch keine Informationen in die Programm-Datenbanken aufgenommen wurden. Dafür wurde eine spezielle Komponente entwickelt, der *Proaktive Schutz*.



Der Proaktive Schutz wurde notwendig, nachdem sich Schadprogramme schneller ausbreiten, als der Virenschutz durch Updates, die zur Neutralisierung dieser Bedrohungen fähig sind, aktualisiert werden kann. Die reaktiven Technologien, auf denen der Virenschutz beruht, erfordern mindestens eine tatsächliche Infektion durch eine neue Bedrohung sowie eine bestimmte Zeit, um den schädlichen Code zu analysieren, die neuen Informationen zu den Programm-Datenbanken hinzuzufügen und diese Datenbanken auf den Benutzercomputern zu aktualisieren. Während dieser Zeit kann eine neue Bedrohung bereits gewaltigen Schaden verursachen.

Durch die präventiven Technologien, auf denen der Proaktive Schutz von Kaspersky Anti-Virus basiert, lässt sich ein solcher Zeitverlust vermeiden und eine neue Bedrohung neutralisieren, noch bevor sie auf Ihrem Computer Schaden verursachen kann. Wie wird das erreicht? Im Unterschied zu den reaktiven Technologien, bei denen die Analyse auf der Basis von Einträgen der Programm-Datenbanken erfolgt, erkennen die Präventivtechnologien eine neue Bedrohung auf Ihrem Computer an der Reihenfolge der Aktionen, die von einem bestimmten Programm ausgeführt werden sollen. Zum Lieferumfang der Anwendung gehört eine Sammlung von Kriterien, mit deren Hilfe sich bestimmen lässt, wie gefährlich die Aktivität eines bestimmten Programms ist. Wenn die Aktions-

reihenfolge eines bestimmten Programms aufgrund der Aktivitätsanalyse einen Verdacht ergibt, wendet Kaspersky Anti-Virus die Aktion an, die in der Regel für eine Aktivität solcher Art festgelegt ist.

Eine gefährliche Aktivität wird durch die Gesamtheit der Programmaktionen charakterisiert. Wenn sich ein bestimmtes Programm beispielsweise selbst in Netzwerkressourcen, in den Autostart-Ordner oder in die Systemregistrierung kopiert und anschließend Kopien verschickt, besteht eine hohe Wahrscheinlichkeit, dass es sich bei diesem Programm um einen Wurm handelt. Als gefährliche Aktivitäten gelten auch:

- Veränderungen des Dateisystems
- Einfügen von Modulen in andere Prozesse
- versteckte Prozesse im System
- Veränderung von bestimmten Schlüsseln der Microsoft Windows-Systemregistrierung

Alle gefährlichen Operationen werden vom Proaktiven Schutz verfolgt und blockiert.

Bei seiner Arbeit verwendet der Proaktive Schutz eine Auswahl von im Lieferumfang der Anwendung enthaltenen Regeln sowie Regeln, die der Benutzer bei der Arbeit mit der Anwendung erstellt. Eine *Regel* ist eine Kombination von Kriterien, welche die Gesamtheit verdächtiger Aktionen und die Reaktion von Kaspersky Anti-Virus auf diese Aktionen festlegen.

Es sind separate Regeln für die Aktivität von Anwendungen, für die Kontrolle von Veränderungen der Systemregistrierung und für auf dem Computer gestartete Programme vorhanden. Sie können die Regeln nach eigenem Ermessen anpassen, Regeln hinzufügen, löschen oder ändern. Es gibt Erlaubnis- und Verbotsregeln.

Der Proaktive Schutz funktioniert nach folgendem Algorithmus:

1. Der Proaktive Schutz analysiert sofort nach dem Start des Computers die folgenden Aspekte:
   - *Aktionen jeder Anwendung, die auf dem Computer gestartet wird*. Der Verlauf der ausgeführten Aktionen und ihre Reihenfolge werden gespeichert und mit der Reihenfolge verglichen, die für eine gefährliche Aktivität charakteristisch ist (Im Lieferumfang von Kaspersky Anti-Virus ist eine Datenbank der Arten von gefährlichen Aktivitäten enthalten, die zusammen mit den Programm-Datenbanken aktualisiert wird).
   - *Integrität der Programm-Module*, der auf Ihrem Computer installierten Anwendungen. Dadurch kann die Veränderung von Anwen-

dungsmodulen und das Einfügen von schädlichem Code in Module verhindert werden.

- *Jeder Versuch zur Veränderung der Systemregistrierung* (Löschen oder Hinzufügen eines Systemregistrierungsschlüssels, Eingabe von Schlüsselwerten in einem ungültigen Format, das Ansicht und Ändern der Schlüssel verhindert, usw.).

2. Die Analyse erfolgt auf der Basis der Erlaubnis- und Verbotsregeln des Proaktiven Schutzes.
3. Als Ergebnis der Analyse sind folgende Varianten für das weitere Vorgehen möglich:

   - Wenn eine Aktivität die Bedingungen einer Erlaubnisregel des Proaktiven Schutzes erfüllt oder nicht unter eine Verbotsregel fällt, wird sie nicht blockiert.
   - Wenn eine Aktivität in einer Verbotsregel beschrieben ist, erfolgt das weitere Vorgehen der Komponente in Übereinstimmung mit der in der Regel festgelegten Aktionsreihenfolge. Gewöhnlich wird eine solche Aktivität blockiert. Auf dem Bildschirm erscheint ein Hinweis, in dem die Anwendung, der Typ ihrer Aktivität und der Verlauf der ausgeführten Aktionen angegeben werden. Sie müssen selbständig eine Entscheidung über Erlaubnis oder Verbot für diese Aktivität fällen. Sie können eine Regel für die Aktivität erstellen und die im System ausgeführten Aktionen rückgängig machen.

     Wenn eine Meldung des Proaktiven Schutzes erfolgt und der Benutzer keine Aktion vornimmt, führt das Programm nach einer bestimmten Zeit die standardmäßig für diese Bedrohung empfohlene Aktion aus. Die empfohlene Aktion kann für die einzelnen Bedrohungstypen unterschiedlich sein.

Der Proaktive Schutz erfolgt genau nach den Parametern (s. Abb. 35), die festlegen:

- *ob die Aktivität der Anwendungen auf Ihrem Computer kontrolliert wird.*

  Dieser Modus des Proaktiven Schutzes wird durch das Kontrollkästchen ☑ **Aktivitätsanalyse aktivieren** geregelt. Der Modus ist standardmäßig aktiviert, wodurch die strenge Analyse der Aktionen jedes Programms gewährleistet wird, das auf Ihrem Computer gestartet werden soll. Für bestimmte Arten gefährlicher Aktivität können Sie die Art der Bearbeitung von Anwendungen (s. Pkt. 10.1 auf S. 135) mit der betreffenden Aktivität festlegen. Außerdem besteht die Möglichkeit, Ausnahmen für den Proaktiven Schutz festzulegen, wodurch die Aktivität der ausgewählten Anwendungen von der Kontrolle ausgeschlossen wird.

- *ob die Kontrolle der Integrität von Anwendungen aktiviert ist.*

Diese Funktionalität ist verantwortlich für die Integrität von Modulen der auf Ihrem Computer installierten Anwendungen und wird durch das Kontrollkästchen **Integritätskontrolle aktivieren** reguliert. Die Integrität wird anhand des Bestands der Module eines Programms und der Kontrollsumme des Abbilds des eigentlichen Programms überwacht. Sie können Regeln (s. Pkt. 10.2 auf S. 139) für die Kontrolle der Integrität von Modulen einer bestimmten Anwendung erstellen. Dazu muss die betreffende Anwendung in die Liste der zu kontrollierenden Anwendungen aufgenommen werden.

Achtung!

Diese Komponente des Proaktiven Schutzes ist nicht in der Anwendung vorhanden, wenn sie auf einem Computer mit dem Betriebssystem Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista oder Microsoft Windows Vista x64 installiert ist.

- *ob die Kontrolle über Veränderungen der Systemregistrierung erfolgt.*

  Das Kontrollkästchen **Überwachung der Systemregistrierung aktivieren** ist standardmäßig aktiviert, was bedeutet, dass Kaspersky Anti-Virus jeden Versuch zur Veränderung eines der Kontrolle unterliegenden Schlüssels in der Systemregistrierung des Betriebssystems Microsoft Windows analysiert.

  Sie können eigene Regeln (s. Pkt. 10.3.2 auf S. 147) zur Kontrolle eines bestimmten Registrierungsschlüssels erstellen.

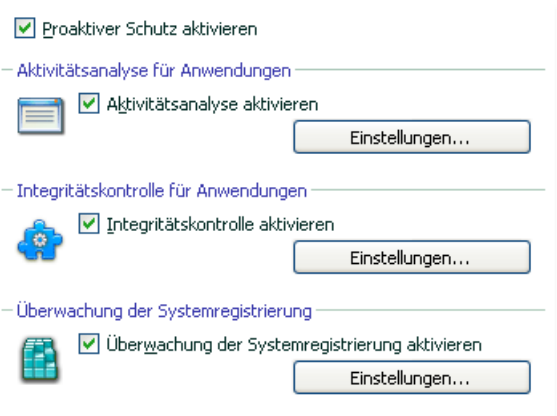


Abbildung 35. Einstellungen für den Proaktiven Schutz

Sie können Ausnahmen für die Module des Proaktiven Schutzes festlegen (s. Pkt. 6.9.1 auf S. 76) und eine Liste der vertrauenswürdigen Anwendungen (s. Pkt. 6.9.2 auf S. 81) erstellen.

Im folgenden Abschnitt des Handbuchs werden alle oben genannten Aspekte ausführlich beschrieben.

10.1. Regeln für die Aktivitätskontrolle

Hinweis

Beachten Sie, dass die Einstellungen für die Aktivitätskontrolle in der Anwendung unterschiedlich sind, je nachdem, ob die Anwendung auf einem Computer mit einem der Betriebssysteme Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista oder Microsoft Windows Vista x64 installiert ist oder auf einem Computer mit anderen Betriebssystemen.

Informationen über die Einstellungen für die Aktivitätskontrolle für die genannten Betriebssysteme finden Sie am Ende dieses Abschnitts.

Die Aktivität der Anwendungen auf Ihrem Computer wird von Kaspersky Anti-Virus kontrolliert. Zum Lieferumfang der Anwendung gehört eine Liste mit Beschreibungen von Ereignissen, die als gefährlich gelten können. Für jedes dieser Ereignisse existiert eine Regel. Wenn die Aktivität einer bestimmten Anwendung als gefährliches Ereignis eingestuft wird, folgt der Proaktive Schutz den Anweisungen, die in der Regel für dieses Ereignis festgelegt sind.

Kreuzen Sie das Kontrollkästchen ☑ **Aktivitätsanalyse aktivieren** an, damit die Aktivität der Anwendungen kontrolliert wird.

Im Folgenden werden einige Arten von Ereignissen beschrieben, die im System eintreten können und von der Anwendung als verdächtig behandelt werden:

- *Gefährliche Aktivität (Verhaltensanalyse)*. Kaspersky Anti-Virus analysiert die Aktivität der Anwendungen, die auf dem Computer installiert sind, und erkennt auf Basis einer Regelliste, die von den Kaspersky-Lab-Spezialisten angelegt wurde, gefährliche und verdächtige Aktionen der Anwendungen. Als solche Aktionen gelten beispielsweise die versteckte Installation eines Programms und das von einem Programm selbst ausgeführte Kopieren.
- *Browserstart mit Parametern*. Die Analyse dieses Aktivitätstyps erlaubt es, Versuche zum versteckten Start eines Browsers mit Parametern zu erkennen. Diese Aktivität ist charakteristisch für den Start eines Web-

browsers aus einer Anwendung mit bestimmten Befehlszeilenschlüsseln: z.B. bei der Verwendung von in einem Werbebrief Ihrer Mailbox enthaltenen Links zu einer bestimmten Adresse im Internet.

- *Eindringen in Prozess*. Hinzufügen von ausführbarem Code zum Prozess eines bestimmten Programms oder Erstellen eines zusätzlichen Datenstroms. Diese Aktivität ist charakteristisch für trojanische Programme.
- *Auftreten eines versteckten Prozesses (Rootkit)*. Ein Rootkit ist eine Auswahl von Programmen, die benutzt werden, um schädliche Programme und ihre Prozesse im System zu tarnen. Kaspersky Anti-Virus analysiert das Betriebssystem auf das Vorhandensein versteckter Prozesse.
- *Eindringen von Fenster-Hooks*. Diese Aktivität wird beim Versuch zum Lesen von Kennwörtern und anderen geheimen Informationen, die in Dialogfenstern des Betriebssystems angezeigt werden, verwendet. Kaspersky Anti-Virus überwacht diese Aktivität beim Versuch des Abfangens von Informationen, die zwischen Betriebssystem und Dialogfenstern ausgetauscht werden.
- *Verdächtige Werte in der Registrierung*. Die Systemregistrierung ist eine Datenbank, in der die System- und Benutzereinstellungen gespeichert sind, welche die Arbeit des Betriebssystems Microsoft Windows sowie der auf dem Computer installierten Dienste regulieren. Schädliche Programme verändern bestimmte Werte in den Registrierungsschlüsseln und versuchen dadurch die eigene Existenz im System zu verheimlichen. Kaspersky Anti-Virus analysiert die Systemregistrierungseinträge auf das Vorhandensein verdächtiger Werte.
- *Verdächtige Aktivität im System*. Die Anwendung analysiert die Aktionen, die vom Betriebssystem Microsoft Windows ausgeführt werden, und erkennt verdächtige Aktivität. Ein Beispiel für verdächtige Aktivität ist eine Integritätsverletzung, die beispielsweise darin bestehen kann, dass ein oder mehrere Module einer kontrollierten Anwendung seit dem vorhergehenden Start verändert wurden.
- *Erkennen von Tastaturspionen*. Diese Aktivität wird von schädlichen Programmen benutzt, um über die Tastatur eingegebene Informationen abzufangen.

Die Liste der gefährlichen Aktivitäten wird beim Update von Kaspersky Anti-Virus automatisch ergänzt und kann nicht verändert werden. Sie können:

- die Kontrolle einer bestimmten Aktivität ablehnen. Deaktivieren Sie dazu das Kontrollkästchen ☑ neben ihrem Namen.

- eine Regel ändern, nach welcher der Proaktive Schutz beim Fund einer gefährlichen Aktivität vorgeht.
- eine Liste von Ausnahmen erstellen (s. Pkt. 6.9 auf S. 75), indem Sie die Anwendungen festlegen, deren Aktivität Sie nicht für gefährlich halten.

Um zur Konfiguration der Aktivitätskontrolle zu wechseln,

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie im Abschnitt **Schutz** die Komponente **Proaktiver Schutz**.
2. Klicken Sie im Block **Aktivitätsanalyse für Anwendungen** (s. Abb. 35) auf die Schaltfläche **Einstellungen**.

Die Arten gefährlicher Aktivität, die vom Proaktiven Schutz kontrolliert werden, werden im Fenster **Einstellungen: Aktivitätsanalyse** genannt (s. Abb. 36).

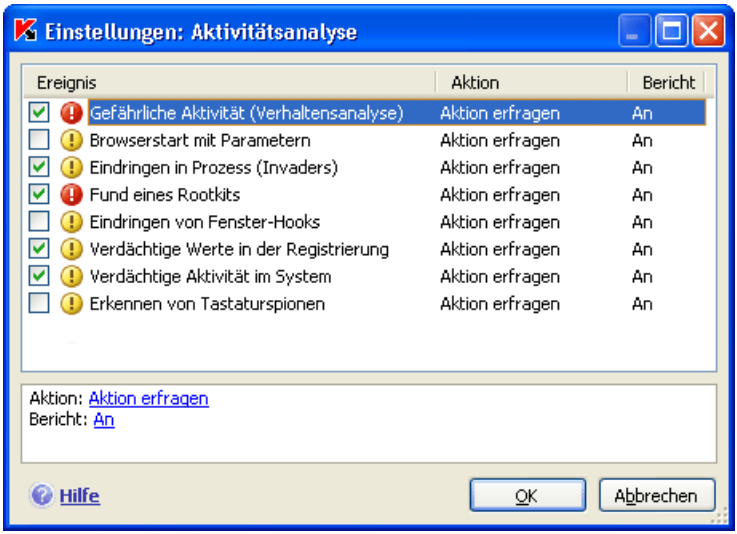


Abbildung 36. Einstellungen für die Aktivitätskontrolle von Anwendungen

Um eine Regel für die Kontrolle einer gefährlichen Aktivität anzupassen, wählen Sie diese in der Liste aus und legen Sie im unteren Teil der Registerkarte die Parameter der Regel fest:

- Wählen Sie die Reaktion des Proaktiven Schutzes auf die gefährliche Aktivität.

  Als Reaktion kann eine der folgenden Aktionen dienen: Erlauben, Aktion erfragen oder Prozess beenden. Klicken Sie mit der linken Maustaste auf den Link mit der Aktion, bis er den gewünschten Wert annimmt. Zu-

sätzlich zum Beenden eines Prozesses kann die Anwendung, die die gefährliche Aktivität initiiert hat, unter Quarantäne gestellt werden. Verwenden Sie dazu den Link An/Aus neben dem entsprechenden Parameter. Für die Suche nach versteckten Prozessen im System können Sie zusätzlich das Intervall angeben, in dem die Untersuchung gestartet werden soll.

- Geben Sie an, ob ein Bericht über die ausgeführte Operation erstellt werden soll. Verwenden Sie dazu den Link An/Aus.

Um die Kontrolle einer bestimmten gefährlichen Aktivität abzulehnen, deaktivieren Sie in der Liste der gefährlichen Aktivitäten das Kontrollkästchen ☑ neben seinem Namen.

Besonderheiten der Einstellungen für die Aktivitätsanalyse von Anwendungen in Kaspersky Anti-Virus unter den Betriebssystemen Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista oder Microsoft Windows Vista x64:

Wenn der Computer unter einem der oben genannten Betriebssystem läuft, wird nur eine Art von Ereignissen kontrolliert, die im System eintreten können: gefährliche Aktivität (Verhaltensanalyse). Damit Kaspersky Anti-Virus zusätzlich auch Veränderungen von Systembenutzerkonten überwacht, aktivieren Sie das Kontrollkästchen ☑ **Systembenutzerkonten kontrollieren** (s. Abb. 37).

Benutzerkonten regulieren den Zugriff auf das System und definieren den Benutzer und seine Arbeitsumgebung. Dadurch werden Beschädigungen des Betriebssystems oder der Daten anderer Benutzer verhindert. Eine gefährliche Aktivität besteht im Verändern von Benutzerkonten (beispielsweise Ändern eines Kennworts).

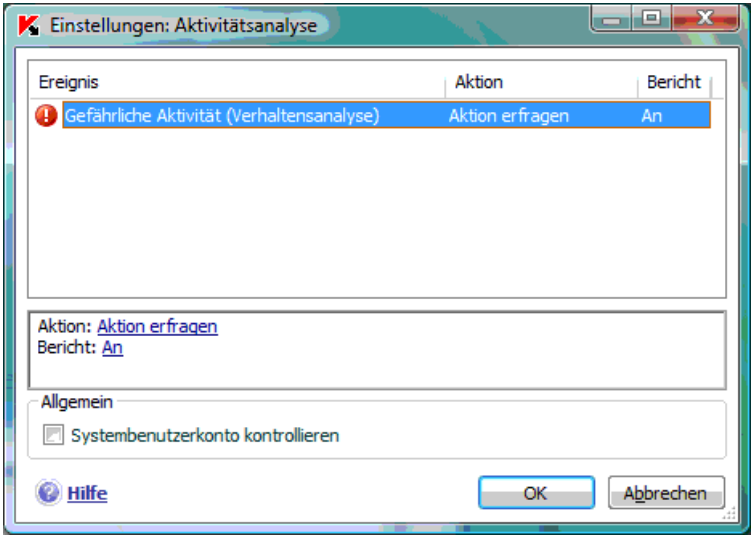


Abbildung 37. Einstellungen für die Aktivitätskontrolle von Anwendungen unter Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64

10.2. Integritätskontrolle für Anwendungen

Achtung!

Diese Komponente des Proaktiven Schutzes funktioniert nicht auf Computern mit dem Betriebssystem Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista oder Microsoft Windows Vista x64.

Es existiert eine Reihe von für das System kritischen Programmen, die von schädlichen Programmen zur Ausbreitung verwendet werden können. Dazu zählen beispielsweise Browser, Mailprogramme sowie Systemanwendungen und Prozesse, die zur Verbindung mit dem Internet und bei der Arbeit mit E-Mails und anderen Dokumenten verwendet werden. Deshalb gelten solche Anwendungen hinsichtlich der Aktivitätskontrolle als *kritisch*.

Der Proaktive Schutz kontrolliert kritische Anwendungen, analysiert ihre Aktivität, die Integrität des Modulbestands dieser Anwendungen und den Start anderer Prozesse durch diese Anwendungen. Im Lieferumfang von Kaspersky Anti-Virus ist eine Liste kritischer Anwendungen enthalten. Für jede kritische Anwendung

existiert eine spezielle Kontrollregel, welche die Aktivität der Anwendung reguliert. Sie können die Liste durch andere Anwendungen, die Ihrer Meinung nach kritisch sind, ergänzen und Regeln für Anwendungen der mitgelieferten Liste löschen oder anpassen.

Neben der Liste kritischer Anwendungen ist auch eine Auswahl vertrauenswürdiger Module vorhanden, die in alle der Kontrolle unterliegenden Anwendungen geladen werden dürfen. Dazu zählen beispielsweise Module, die über eine Signatur der Microsoft Corporation verfügen. Die Aktivität von Anwendungen, zu denen diese Module gehören, ist mit hoher Wahrscheinlichkeit unschädlich, weshalb eine strenge Kontrolle über die Aktionen nicht erforderlich ist. Die Kaspersky-Lab-Spezialisten haben eine Liste dieser Module erstellt, um die Belastung Ihres Computers bei der Arbeit des Proaktiven Schutzes zu verringern.

In der Grundeinstellung werden Komponenten, die eine Signatur der Microsoft Corporation besitzen, automatisch zur Liste der vertrauenswürdigen Anwendungen hinzugefügt. Bei Bedarf können Sie Komponenten zur Liste hinzufügen oder daraus entfernen.

Die Kontrolle über Systemprozesse wird durch das Kontrollkästchen **Integritätskontrolle aktivieren** reguliert. Das Kontrollkästchen ist standardmäßig deaktiviert. Wenn die Integritätskontrolle aktiv ist, wird jede Anwendung bzw. Anwendungsmodul, die/das gestartet werden sollen, auf Zugehörigkeit zur Liste der kritischen oder vertrauenswürdigen Anwendungen geprüft. Wenn eine Anwendung auf der Liste der kritischen Anwendungen steht, wird ihre Aktivität der Kontrolle durch den Proaktiven Schutz unterzogen, wozu die dafür erstellte Regel dient.

Um zur Konfiguration der Prozessüberwachung zu wechseln,

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie im Abschnitt **Schutz** die Komponente **Proaktiver Schutz**.
2. Klicken Sie im Block **Integritätskontrolle für Anwendungen** (s. Abb. 35) auf die Schaltfläche **Einstellungen**.

Im Folgenden wird die Arbeit mit kritischen und vertrauenswürdigen Prozessen genauer beschrieben.

10.2.1. Konfiguration von Kontrollregeln für kritische Anwendungen

Kritische Anwendungen sind ausführbare Programmdateien, deren Aktivitätskontrolle von hoher Bedeutung ist, weil solche Programme von schädlichen Objekten verwendet werden können, um sich selbst auszubreiten.

Eine Liste kritischer Anwendungen befindet sich auf der Registerkarte **Zu überwachende Anwendungen** (s. Abb. 38). Diese Liste wurde von den Kaspersky-Lab-Spezialisten erstellt und gehört zum Lieferumfang der Anwendung. Für jede kritische Anwendung gibt es eine Kontrollregel, welche die Aktivität dieser Anwendung reguliert. Sie können die vorhandenen Regeln anpassen und eigene Regeln erstellen.

Der Proaktive Schutz analysiert folgende Operationen mit kritischen Anwendungen: Start, Ändern der Zusammensetzung von Anwendungsmodulen und Start einer Anwendung als untergeordneter Prozess. Für jede der genannten Operationen können Sie eine Reaktion des Proaktiven Schutzes wählen (Operation erlauben oder verbieten). Außerdem kann festgelegt werden, ob die Aktivität in einem Bericht über die Arbeit der Komponente festgehalten werden soll. Standardmäßig werden praktisch für alle kritischen Anwendungen die Operationen zum Starten, Ändern oder Starten von untergeordneten Prozessen erlaubt.

Um eine Anwendung zur Liste der kritischen Anwendungen hinzuzufügen und eine Regel dafür zu erstellen,

1. Klicken Sie auf der Registerkarte **Zu überwachende Anwendungen** auf die Schaltfläche **Hinzufügen**. Dadurch öffnet sich das Kontextmenü, in dem Sie mit dem Punkt **Durchsuchen** in das Standardfenster zur Dateiauswahl oder mit dem Punkt **Anwendungen** zur Liste der momentan laufenden Anwendungen gelangen, um die gewünschte Anwendung auszuwählen. Die Anwendung wird der Liste an erste Stelle hinzugefügt. Standardmäßig wird eine Erlaubnisregel für sie erstellt. Beim ersten Start dieser Anwendung wird eine Liste der während des Starts benutzten Module angelegt. Diese Module werden erlaubt.

2. Markieren Sie die Regel in der Liste und legen Sie im unteren Teil der Registerkarte die Parameter der Regel fest:

   - Bestimmen Sie, wie der Proaktive Schutz reagieren soll, wenn versucht wird, die kritische Anwendung zu starten, ihre Module zu verändern oder eine kritische Anwendung als untergeordneten Prozess zu starten.

     Als Reaktion stehen folgende Aktionen zur Auswahl: erlauben, Aktion erfragen und verbieten. Klicken Sie mit der linken Maustaste auf den Link mit der Aktion, bis er den gewünschten Wert annimmt.

   - Legen Sie fest, ob ein Bericht über die ausgeführte Operation erstellt werden soll. Verwenden Sie dazu den Link protokollieren/nicht protokollieren.

Um die Kontrolle über die Aktivität einer bestimmten Anwendung abzulehnen, deaktivieren Sie neben ihrem Namen das Kontrollkästchen ☑.

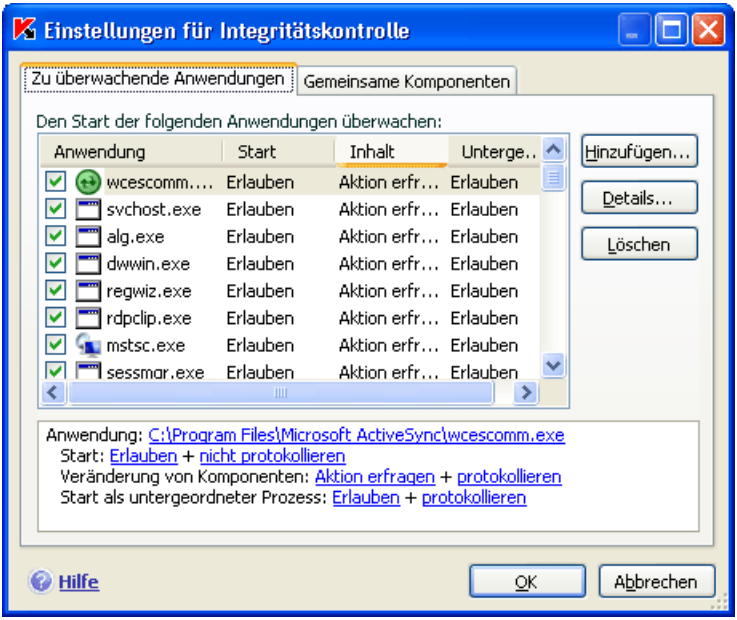


Abbildung 38. Einstellungen für die Integritätskontrolle für Anwendungen

Verwenden Sie die Schaltfläche **Details**, um Details für die Liste der Module der gewählten Anwendung anzuzeigen. Das folgende Fenster **Einstellungen: Anwendungsmodule** enthält eine Liste der Module, die zur zu kontrollierenden Anwendung gehören und bei ihrem Start verwendet werden. Sie können die Liste mit Hilfe der Schaltflächen **Hinzufügen** und **Löschen** bearbeiten. Die Schaltflächen befinden sich auf der rechten Seite des Fensters.

Außerdem können Sie erlauben oder verbieten, dass ein bestimmtes Modul von der zu kontrollierenden Anwendung geladen wird. Standardmäßig wird für jedes Modul eine Erlaubnisregel erstellt. Um die Aktion zu ändern, markieren Sie das Modul in der Liste, klicken Sie auf **Ändern** und legen Sie im folgenden Fenster die gewünschte Aktion fest.

Achtung!

Beachten Sie, dass ein Trainingsvorgang ausgeführt wird, wenn eine zu kontrollierende Anwendung nach der Installation von Kaspersky Anti-Virus zum ersten Mal gestartet wird. Das Training dauert an, bis die Arbeit der Anwendung beendet wird. Während des Trainings wird eine Liste der von der Anwendung verwendeten Module erstellt. Die Regeln zur Integritätskontrolle werden bei den nachfolgenden Starts der Anwendung verwendet.

10.2.2. Erstellen einer Liste der gemeinsamen Komponenten

Kaspersky Anti-Virus verfügt über eine Liste von gemeinsamen Komponenten, die in alle zu kontrollierenden Anwendungen geladen werden dürfen. Diese Liste befindet sich auf der Registerkarte **Gemeinsame Komponenten** (s. Abb. 39). Die Liste enthält Module, die von Kaspersky Anti-Virus verwendet werden, Komponenten, die über eine Microsoft Corporation-Signatur verfügen, sowie vom Benutzer hinzugefügte Komponenten.

Abbildung 39. Anpassen der Liste mit vertrauenswürdigen Modulen

Damit die Module von Programmen, die Sie auf Ihrem Computer installieren und die über eine Microsoft Corporation-Signatur verfügen, automatisch zur Liste der vertrauenswürdigen Module hinzugefügt werden, aktivieren Sie das Kontrollkästchen ☑ **Komponenten mit Microsoft Corporation Signatur automatisch zur Liste hinzufügen**. Wenn in diesem Fall eine der Kontrolle unterliegende Anwendung versucht, ein Modul zu laden, das eine Microsoft Corporation-Signatur besitzt, wird das Laden dieses Moduls automatisch erlaubt und das Modul wird zur Liste der gemeinsamen Komponenten hinzugefügt.

Um der Liste ein vertrauenswürdiges Modul hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen** und wählen Sie im Standardfenster zur Dateiauswahl das Modul.

10.3. Kontrolle über Veränderungen der Systemregistrierung

Ein Ziel vieler schädlicher Programme besteht in einer Veränderung der Registrierung des Betriebssystems auf Ihrem Computer. Dabei kann es sich um harmlose Scherzprogramme oder aber um gefährliche Schadprogramme handeln, die eine ernste Bedrohung für Ihren Computer darstellen.

Schädliche Programme können beispielsweise ihren Start in einen Registrierungsschlüssel eintragen, der dem automatischen Start von Anwendungen dient. Dadurch wird das schädliche Programm gleich nach dem Start des Betriebssystems automatisch gestartet.

Ein spezielles Modul des Proaktiven Schutzes überwacht die Veränderungen von Systemregistrierungsobjekten. Die Arbeit dieses Moduls wird durch das Kontrollkästchen ☑ **Überwachung der Systemregistrierung aktivieren** reguliert.

Um zur Konfiguration der Systemregistrierungskontrolle zu wechseln,

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie im Abschnitt **Schutz** die Komponente **Proaktiver Schutz**.
2. Klicken Sie im Block **Überwachung der Systemregistrierung** (s. Abb. 35) auf die Schaltfläche **Einstellungen**

Eine Liste der Regeln für die Arbeit mit Registrierungsobjekten wurde bereits von den Kaspersky-Lab-Spezialisten erstellt und gehört zum Lieferumfang des Programms. Die Operationen mit den Registrierungsobjekten sind in logische Gruppen wie *System Security, Internet Security usw.* unterteilt. Jede Gruppe enthält Objekte der Systemregistrierung und Regeln für die Arbeit mit diesen. Die Liste wird zusammen mit dem Programm-Update aktualisiert.

Eine vollständige Liste der Regeln befindet sich im Fenster **Gruppen der Registrierungsschlüssel** (s. Abb. 40).

Jede Regelgruppe besitzt eine bestimmte Ausführungspriorität, die Sie mit Hilfe der Schaltflächen **Aufwärts** und **Abwärts** erhöhen oder vermindern können. Je höher die Position einer Gruppe in der Liste, desto höher ist ihre Ausführungspriorität. Wenn ein Registrierungsobjekt zu mehreren Gruppen gehört, wird zuerst die Regel aus der Gruppe mit der höchsten Priorität auf das Objekt angewandt.

Die Verwendung einer bestimmten Regelgruppe kann folgendermaßen aufgehoben werden:

- Deaktivieren des Kontrollkästchens ☑ neben dem Namen der Gruppe. In diesem Fall verbleibt die Regelgruppe in der Liste, wird aber nicht verwendet.
- Löschen der Regelgruppe aus der Liste. Es wird davor gewarnt, die von den Kaspersky-Lab-Spezialisten erstellten Gruppen zu löschen, weil sie eine Liste der Systemregistrierungsobjekte enthalten, die am häufigsten von Schadprogrammen benutzt werden.

Es besteht die Möglichkeit, eigene Gruppen für zu kontrollierende Systemregistrierungsobjekte zu erstellen. Klicken Sie dazu im Fenster der Objektgruppen auf die Schaltfläche **Hinzufügen**.

Nehmen Sie im nächsten Fenster folgende Einstellungen vor:

1. Geben Sie den Namen der neuen Gruppe von Systemregistrierungsobjekten im Feld **Gruppenname** an.
2. Erstellen Sie eine Liste mit den Objekten der Systemregistrierung, die der zu kontrollierenden Gruppe angehören sollen. Dazu dient die Registerkarte **Schlüssel** (s. Pkt. 10.3.1 auf S. 146). Dabei können ein oder mehrere Objekte verwendet werden.
3. Erstellen Sie eine Regel für die Objekte der Registrierung. Dazu dient die Registerkarte **Regeln** (s. Pkt. 10.3.2 auf S. 147). Sie können mehrere Regeln erstellen und ihre Anwendungspriorität bestimmen.

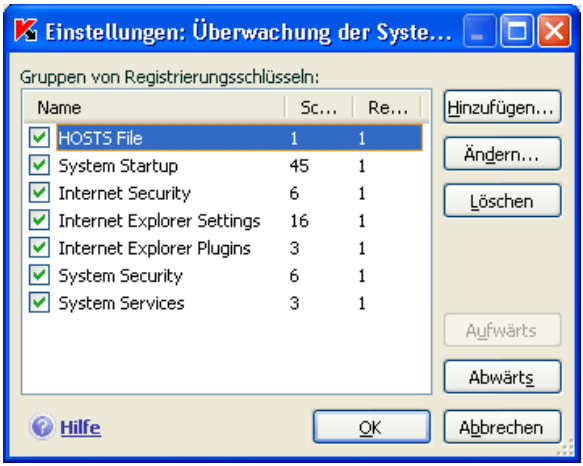


Abbildung 40. Zu kontrollierende Schlüssel der Systemregistrierung

10.3.1. Auswahl von Registrierungsobjekten zum Erstellen einer Regel

Die erstellte Gruppe von Objekten muss mindestens ein Systemregistrierungsobjekt enthalten. Die Liste der Objekte für die Regel wird auf der Registerkarte **Schlüssel** angelegt.

Um ein Systemregistrierungsobjekt hinzuzufügen,

1. Klicken Sie im Fenster **Gruppe ändern** auf die Schaltfläche **Hinzufügen** (s. Abb. 41).
2. Wählen Sie im folgenden Fenster das Objekt oder die Gruppe von Objekten der Systemregistrierung, für die Sie eine Kontrollregel erstellen möchten.
3. Geben Sie im Feld **Wert** den Wert des Objekts oder die Maske der Gruppe von Objekten an, für welche(s) die Regel gelten soll.
4. Aktivieren Sie das Kontrollkästchen **Untergeordnete Schlüssel einschließen**, damit die Regel auf alle untergeordneten Schlüssel des gewählten Systemregistrierungsobjekts angewandt wird.

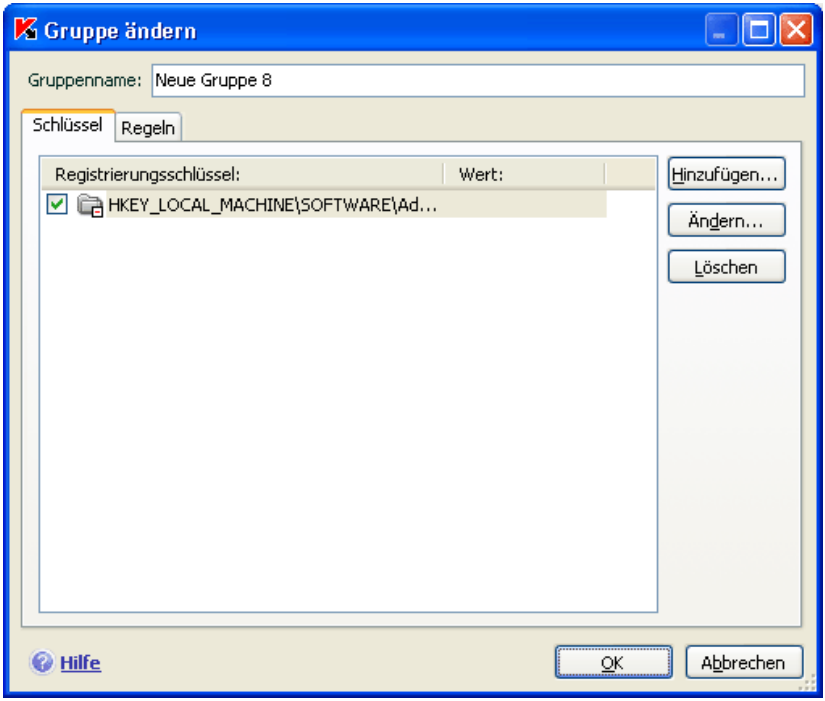


Abbildung 41. Hinzufügen eines Registrierungsschlüssels, der kontrolliert werden soll

Achtung!

Eine Maske mit den Zeichen * oder ? muss nur dann gleichzeitig mit dem Kontrollkästchen **Untergeordnete Schlüssel einschließen** verwendet werden, wenn diese Zeichen im Namen des Schlüssels vorhanden sind.

Wenn eine Gruppe von Registrierungsobjekten mit Hilfe einer Maske ausgewählt und dafür ein konkreter Wert angegeben wurde, wird die Regel streng auf den angegebenen Wert für jeden beliebigen Schlüssel der gewählten Gruppe angewandt.

10.3.2. Erstellen einer Regel zur Kontrolle von Registrierungsobjekten

Eine Kontrollregel für Systemregistrierungsobjekte besteht aus folgenden Parametern:

- Anwendung, für welche die Regel benutzt wird, wenn sie versucht, auf Systemregistrierungsobjekte zuzugreifen.
- Reaktion des Programms auf den Versuch der Anwendung, eine bestimmte Operation mit Systemregistrierungsobjekten auszuführen.

Um eine Regel für die ausgewählten Systemregistrierungsobjekte zu erstellen,

1. Klicken Sie auf der Registerkarte **Regeln** auf die Schaltfläche **Erstellen**. Die vordefinierte Regel wird an erster Stelle zur Regelliste hinzugefügt (s. Abb. 42).
2. Markieren Sie die Regel in der Liste und legen Sie im unteren Bereich der Registerkarte die Parameter der Regel fest:
   - Geben Sie eine Anwendung an.

     Die Regel wird standardmäßig für eine beliebige Anwendung erstellt. Damit sich die Regel auf eine konkrete Anwendung bezieht, klicken Sie mit der linken Maustaste auf den Link Beliebige, der dadurch den Wert Ausgewählte annimmt. Verwenden Sie dann den Link Anwendung angeben. Dadurch öffnet sich ein Kontextmenü, in dem Sie mit dem Punkt **Durchsuchen** in das Standardfenster zur Dateiauswahl oder mit dem Punkt **Anwendungen** zur Liste der momentan aktiven Anwendungen wechseln können, um die gewünschte Anwendung auszuwählen.
   - Bestimmen Sie die Reaktion des Proaktiven Schutzes auf den Versuch der gewählten Anwendung, eine Operation zum Lesen, Ändern oder Löschen von Systemregistrierungsobjekten auszuführen.

     Als Reaktion kann eine der folgenden Aktionen verwendet werden: erlauben, Aktion erfragen und verbieten. Klicken Sie mit der linken Maustaste auf den Link mit der Aktion, bis er den gewünschten Wert annimmt.
   - Legen Sie fest, ob ein Bericht über die ausgeführte Operation erstellt werden soll. Verwenden Sie dazu den Link protokollieren/nicht protokollieren.

Sie können mehrere Regeln erstellen und deren Ausführungspriorität mit Hilfe der Schaltflächen **Aufwärts** und **Abwärts** festlegen. Je höher die Position einer Regel in der Liste, desto höher ist ihre Priorität.

Eine Erlaubnisregel für ein Systemregistrierungsobjekt kann auch aus der Meldung erstellt werden, die bei einer versuchten Operation mit dem Objekt erscheint. Verwenden Sie dazu in der Meldung den Link Erlaubnisregel erstellen und geben Sie im folgenden Fenster das Systemregistrierungsobjekt an, auf das sich die Regel beziehen soll.

Abbildung 42. Erstellen einer Kontrollregel für Systemregistrierungsschlüssel

KAPITEL 11. VIRENSUCHE AUF DEM COMPUTER

Ein wichtiger Bestandteil des Antiviren-Schutzes für einen Computer ist die Virensuche in vom Benutzer festgelegten Bereichen. Kaspersky Anti-Virus 7.0 erlaubt es, sowohl einzelne Objekte (Dateien, Ordner, Laufwerke, Wechseldatenträger) als auch den gesamten Computer auf das Vorhandensein von Viren zu untersuchen. Durch die Virensuche lässt sich die Möglichkeit der Ausbreitung eines schädlichen Codes verhindern, der von den Echtzeitschutz-Komponenten aus bestimmten Gründen nicht erkannt wurde.

Kaspersky Anti-Virus 7.0 verfügt über folgende standardmäßigen Aufgaben zur Virensuche:

Kritische Bereiche

Virenuntersuchung aller kritischen Computerbereiche, sowie Virenuntersuchung aller Objekte, die am Systemstart beteiligt sind. Dazu gehören: Systemspeicher, Objekte, die beim Systemstart gestartet werden, Laufwerksbootsektoren und *Windows*-Systemverzeichnisse. Das Ziel dieser Aufgabe besteht im schnellen Auffinden von im System aktiven Viren, ohne dazu die vollständige Untersuchung des Computers zu starten.

Arbeitsplatz

Virensuche auf Ihrem Computer mit sorgfältiger Untersuchung aller angeschlossenen Laufwerke, des Arbeitsspeichers und der Dateien.

Autostart-Objekte

Virenuntersuchung der Objekte, die beim Start des Betriebssystems geladen werden.

Rootkits

Der Computer wird nach Rootkits durchsucht. Rootkits verstecken schädliche Programme im Betriebssystem. Diese Utilities dringen ins System ein, tarnen ihre Existenz sowie die Existenz von in der Konfiguration des Rootkits beschriebener Malware, die sich in Prozessen, Ordnern oder Registrierungsschlüsseln des Systems befinden kann.

Diese Aufgaben werden standardmäßig mit den empfohlenen Schutzeinstellungen ausgeführt. Sie können diese Einstellungen ändern (s. Pkt. 11.4 auf S. 155) und einen Zeitplan für den Aufgabenstart festlegen (s. Pkt. 6.7 auf S. 71).

Außerdem besteht die Möglichkeit, eigene Aufgaben zur Virensuche zu erstellen (s. Pkt. 11.3 auf S. 153) und einen Startzeitplan dafür anzulegen. Es kann beispielsweise eine Aufgabe zur wöchentlichen Untersuchung von Mailboxen oder eine Aufgabe zur Virensuche im Ordner **Eigene Dateien** erstellt werden.

Daneben können Sie ein beliebiges Objekt auf Viren untersuchen (z.B. eine Festplatte, auf der sich Programme und Spiele befinden, Mail-Datenbanken, die aus dem Büro mitgebracht wurden, ein Archiv, das per E-Mail empfangen wurde, usw.), ohne dafür eine spezielle Untersuchungsaufgabe zu erstellen. Das zu untersuchende Objekt kann aus dem Interface von Kaspersky Anti-Virus 7.0 oder mit den Standardmitteln von Microsoft Windows (beispielsweise im Fenster des Programms **Explorer** oder auf dem **Arbeitsplatz** usw.) ausgewählt werden.

Eine vollständige Liste der Aufgaben zur Virensuche, die für Ihren Computer erstellt wurden, kann im Abschnitt **Virensuche** auf der linken Seite des Programmhauptfensters angezeigt werden.

Sie können eine Notfall-CD zur Systemwiederherstellung erstellen (s. 15.4 auf S. 204), die dazu dient, das System wiederherzustellen, wenn nach einem Virenangriff die Dateien des Betriebssystems beschädigt sind und sich der Computer nicht mehr hochfahren lässt. Verwenden Sie dazu den Link Notfall-CD erstellen.

11.1. Steuerung von Aufgaben zur Virensuche

Der Start von Aufgaben zur Virensuche erfolgt entweder manuell oder automatisch nach einem festgelegten Zeitplan (s. Pkt. 6.7 auf S. 71).

Um eine Untersuchungsaufgabe manuell zu starten,

wählen Sie im Abschnitt **Virensuche** des Programmhauptfensters den Aufgabennamen und verwenden Sie den Link Untersuchung starten.

Momentan ausgeführte Aufgaben werden im Kontextmenü angezeigt, das durch Rechtsklick auf das Programmsymbol im Infobereich der Taskleiste von Microsoft Windows geöffnet wird.

Um eine Untersuchungsaufgabe anzuhalten,

wählen Sie den Namen der Aufgabe im Abschnitt **Virensuche** des Programmhauptfensters und verwenden Sie den Befehl Pause. Die Untersuchung wird angehalten, bis die Aufgabe manuell oder nach Zeitplan erneut gestartet wird. Verwenden Sie den Link Fortsetzen, um die Untersuchung manuell zu starten.

Um die Ausführung einer Aufgabe zu beenden,

wählen Sie den Namen der Aufgabe im Abschnitt **Virensuche** des Programmhauptfensters und verwenden Sie den Befehl Stopp. Die Untersuchung wird angehalten, bis die Aufgabe manuell oder nach Zeitplan erneut gestartet wird. Beim folgenden Start der Aufgabe wird Ihnen vorgeschlagen, die abgebrochene Untersuchung fortzusetzen oder erneut zu beginnen.

11.2. Erstellen einer Liste der Untersuchungsobjekte

Um eine Liste der Objekte anzuzeigen, die bei der Ausführung dieser Aufgabe untersucht werden, wählen Sie im Abschnitt **Virensuche** des Programmhauptfensters den Namen einer Aufgabe (z.B. **Arbeitsplatz**). Die Liste der Objekte wird auf der rechten Seite des Fensters angezeigt (s. Abb. 43).

Abbildung 43. Liste der Untersuchungsobjekte

Für Aufgaben, die standardmäßig bei der Programminstallation erstellt wurden, besteht bereits eine Liste der zu untersuchenden Objekte. Beim Erstellen eigener Aufgaben oder bei der Auswahl eines Objekts im Rahmen einer Aufgabe zur Virenuntersuchung eines separaten Objekts erstellen Sie die Liste der Objekte selbst.

Zum Ergänzen und Ändern der Liste der Untersuchungsobjekte dienen die Schaltflächen, die rechts von der Liste angebracht sind. Klicken Sie auf die Schaltfläche **Hinzufügen**, um der Liste ein neues Untersuchungsobjekt hinzuzufügen und geben Sie im folgenden Fenster das Untersuchungsobjekt an.

Aus Gründen der Bedienungsfreundlichkeit können dem Untersuchungsbereich solche Kategorien wie Mailboxen des Benutzers, Systemspeicher, Autostart-Objekte, Sicherungsdateien des Betriebssystems, und Objekte, die sich im Quarantäneordner von Kaspersky Anti-Virus befinden, hinzugefügt werden.

Außerdem kann beim Hinzufügen eines Ordners, der untergeordnete Objekte enthält, die Option zur rekursiven Untersuchung geändert werden. Wählen Sie dazu das Objekt in der Liste der Untersuchungsobjekte aus, öffnen Sie das Kontextmenü und verwenden Sie den Befehl **Unterordner einschließen**.

Um ein Objekt zu löschen, markieren Sie es in der Liste (dabei wird der Objektname durch grauen Hintergrund hervorgehoben) und klicken Sie auf die Schaltfläche **Löschen**. Sie können die Untersuchung einzelner Objekte bei der Ausführung einer bestimmten Aufgabe vorübergehend ausschalten, ohne die Objekte aus der Liste zu löschen. Deaktivieren Sie dazu einfach das Kontrollkästchen neben dem Objekt, das nicht untersucht werden soll.

Klicken Sie zum Starten einer Untersuchungsaufgabe auf den Link Untersuchung starten.

Außerdem können Sie ein Untersuchungsobjekt mit den Standardmitteln des Betriebssystems Microsoft Windows (beispielsweise im Fenster des Programms **Explorer** oder auf dem **Arbeitsplatz** usw.) auswählen (s. Abb. 44). Führen Sie dazu den Mauszeiger auf den Namen des gewünschten Objekts, öffnen Sie mit der rechten Maustaste das Microsoft Windows-Kontextmenü und wählen Sie den Punkt **Auf Viren untersuchen**.

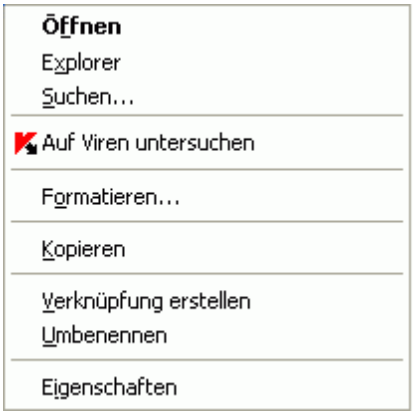


Abbildung 44. Untersuchung eines Objekts aus dem Kontextmenü von Microsoft Windows

11.3. Erstellen von Aufgaben zur Virensuche

Zur Virenuntersuchung von Objekten Ihres Computers können Sie die vordefinierten Untersuchungsaufgaben verwenden, die zum Lieferumfang des Prog-

ramms gehören, sowie eigene Aufgaben erstellen. Eine neue Aufgabe wird auf der Basis von bereits vorhandenen Untersuchungsaufgaben erstellt.

Um eine neue Untersuchungsaufgabe zu erstellen,

1. Wählen Sie im Abschnitt **Virensuche** des Programmhauptfensters die Aufgabe, deren Parameter Ihren Anforderungen am nächsten kommen.
2. Öffnen Sie das Kontextmenü und wählen Sie den Punkt **Speichern unter** oder verwenden Sie den Link Neue Untersuchungsaufgabe.
3. Geben Sie im folgenden Fenster den Namen der neuen Aufgabe an und klicken Sie auf die Schaltfläche **OK**. Danach erscheint die Aufgabe mit dem festgelegten Namen in der Aufgabenliste des Abschnitts **Virensuche** im Programmhauptfenster.

Achtung!

Der Benutzer kann maximal vier Aufgaben erstellen.

Eine neu erstellte Aufgabe erbt alle Parameter der Aufgabe, auf deren Basis sie erstellt wurde. Deshalb ist die zusätzliche Konfiguration erforderlich: Erstellen Sie eine Liste der Untersuchungsobjekte (s. Pkt. 11.2 auf S. 152), legen Sie die Parameter fest (s. Pkt. 11.4 auf S. 155), mit denen die Aufgabe ausgeführt werden soll, und erstellen Sie den Zeitplan für den automatischen Start (s. Pkt. 6.7 auf S. 71).

Um eine erstellte Aufgabe umzubenennen,

wählen Sie die Aufgabe im Abschnitt **Virensuche** des Programmhauptfensters und verwenden Sie den Link Umbenennen.

Geben Sie im folgenden Fenster den neuen Namen für die Aufgabe an und klicken Sie auf die Schaltfläche **OK**. Dadurch wird der Aufgabenname im Abschnitt **Virensuche** geändert.

Um eine erstellte Aufgabe zu löschen,

wählen Sie die Aufgabe im Abschnitt **Virensuche** des Programmhauptfensters und verwenden Sie den Link Löschen.

Bestätigen Sie im Bestätigungsfenster, dass die Aufgabe gelöscht werden soll. Dadurch wird die Aufgabe aus der Aufgabenliste im Abschnitt **Virensuche** gelöscht.

Achtung!

Nur Aufgaben, die von Ihnen selbst erstellt wurden, können umbenannt und gelöscht werden.

11.4. Konfiguration von Aufgaben zur Virensuche

Auf welche Weise die Untersuchung von Objekten auf Ihrem Computer erfolgt, wird durch eine Auswahl von Parametern bestimmt, die für jede Aufgabe festgelegt werden.

Um zur Konfiguration der Aufgabenparameter zu wechseln,

öffnen Sie das Konfigurationsfenster des Programms, wählen Sie im Abschnitt **Virensuche** den Namen der Aufgabe und verwenden Sie den Link Anpassen.

Im Konfigurationsfenster können Sie für jede der Aufgaben:

- die Sicherheitsstufe wählen, auf deren Basis die Aufgabe ausgeführt werden soll (s. Pkt. 11.4.1 auf S. 156).
- zur detaillierten Konfiguration der Stufe wechseln:
  - die Parameter angeben, welche die Dateitypen bestimmen, die der Virenanalyse unterzogen werden (s. Pkt. 11.4.2 auf S. 157).
  - den Start von Aufgaben unter einem anderen Benutzerkonto konfigurieren (s. Pkt. 6.6 auf S. 70).
  - zusätzliche Parameter für die Untersuchung angeben (s. Pkt. 11.4.3 auf S. 160).
  - die Suche nach Rootkits (s. Pkt. 11.4.4 auf S. 162) und die Verwendung von heuristischen Analysemethoden (s. Pkt. 11.4.5 auf S. 164) aktivieren.
- die standardmäßig verwendeten Untersuchungsparameter wiederherstellen (s. Pkt. 11.4.6 auf S. 164).
- die Aktion wählen, die vom Programm beim Fund eines infizierten bzw. möglicherweise infizierten Objekts angewandt wird (s. Pkt. 11.4.7 auf S. 165).
- einen Zeitplan für den automatischen Aufgabenstart erstellen (s. Pkt. 6.7 auf S. 71).

Außerdem können Sie einheitliche Parameter für den Start aller Aufgaben festlegen (s. Pkt. 11.4.8 auf S. 167).

Im Folgenden werden alle oben aufgezählten Parameter zur Konfiguration einer Aufgabe ausführlich beschrieben.

11.4.1. Auswahl der Sicherheitsstufe

Jede Aufgabe zur Virensuche gewährleistet die Untersuchung von Objekten auf einer der folgenden Stufen (s. Abb. 45):

Maximaler Schutz – Untersuchung des gesamten Computers oder eines Laufwerks, Ordners oder einer Datei mit maximaler Ausführlichkeit. Die Verwendung dieser Stufe wird empfohlen, wenn der Verdacht auf eine Virusinfektion Ihres Computers besteht.

Empfohlen – Die Parameter dieser Stufe entsprechen den von den Kaspersky-Lab-Experten empfohlenen Einstellungen. Sie umfassen die Untersuchung der gleichen Objekte wie auf der Stufe **Maximaler Schutz** unter Ausnahme von Dateien in Mailformaten.

Maximales Tempo – Da die Auswahl der untersuchten Dateien auf dieser Stufe eingeschränkt wird, erlaubt Ihnen diese Stufe, komfortabel mit Anwendungen zu arbeiten, die den Arbeitsspeicher stark beanspruchen.

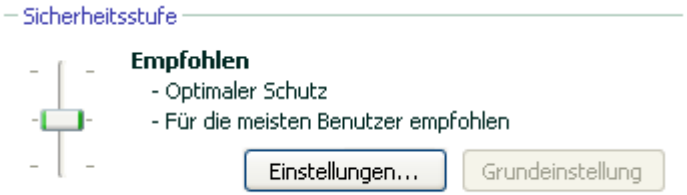


Abbildung 45. Auswahl der Sicherheitsstufe für die Virenuntersuchung von Objekten

Die Untersuchung von Objekten erfolgt standardmäßig auf der **Empfohlenen** Stufe.

Sie können die Stufe für die Untersuchung von Dateien erhöhen oder senken, indem Sie eine andere Stufe wählen oder die Einstellungen der aktuellen Stufe ändern.

Um die Sicherheitsstufe zu ändern,

verschieben Sie den Zeiger auf der Skala. Durch das Anpassen der Sicherheitsstufe wird das Verhältnis zwischen der Ausführungsgeschwindigkeit der Untersuchung und der Anzahl der zu untersuchenden Dateien bestimmt: Je weniger Dateien der Virenanalyse unterzogen werden, desto höher ist die Untersuchungsgeschwindigkeit.

Wenn eine der genannten Sicherheitsstufen für die Untersuchung nicht vollständig Ihren Anforderungen entspricht, können Sie die Untersuchungsparameter zusätzlich anpassen. Wählen Sie dazu die Stufe, die Ihren Anforderungen am

nächsten kommt, als Ausgangsstufe und ändern Sie ihre Parameter entsprechend. In diesem Fall ändert sich der Name der Sicherheitsstufe in **Benutzerdefiniert**.

Um die Einstellungen der aktuellen Sicherheitsstufe anzupassen,

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie den Abschnitt **Virensuche**.
2. Klicken Sie im Block **Sicherheitsstufe** (s. Abb. 45) auf die Schaltfläche **Einstellungen**.
3. Passen Sie im folgenden Fenster die Untersuchungsparameter an und klicken Sie auf **OK**.

11.4.2. Festlegen der zu untersuchenden Objekttypen

Durch die Angabe der Typen der zu untersuchenden Objekte bestimmen Sie das Format, die Größe und die Laufwerke der Dateien die beim Ausführen dieser Aufgabe untersucht werden sollen.

Der Typ der zu untersuchenden Dateien wird im Abschnitt **Dateitypen** festgelegt (s. Abb. 46). Wählen Sie eine der drei Varianten:

- **Alle Dateien untersuchen**. In diesem Fall werden alle Dateien ohne Ausnahme der Untersuchung unterzogen.
- **Programme und Dokumente (nach Inhalt) untersuchen**. Bei der Auswahl dieser Gruppe untersucht das Programm nur potentiell infizierbare Dateien, d.h. Dateien, in die ein Virus eindringen kann.

  Hinweis

  Es gibt eine Reihe von Dateiformaten, für die das Risiko des Eindringens von schädlichem Code und der späteren Aktivierung relativ gering ist. Dazu zählen beispielsweise Dateien im *txt*-Format.

  Im Gegensatz dazu gibt es Dateiformate, die ausführbaren Code enthalten oder enthalten können. Als Beispiele für solche Objekte dienen Dateien der Formate *exe*, *dll*, *doc*. Das Risiko des Eindringens und der Aktivierung von schädlichem Code ist für solche Dateien relativ hoch.

  Bevor die Virensuche in einem Objekt beginnt, wird die interne Kopfzeile des Objekts hinsichtlich des Dateiformats analysiert (txt, doc, exe usw.).

Abbildung 46. Untersuchungseinstellungen

Programme und Dokumente (nach Erweiterung) untersuchen. In diesem Fall untersucht das Programm nur potentiell infizierbare Dateien, wobei das Dateiformat auf Basis der Dateinamenserweiterung ermittelt wird. Wenn Sie dem Link Erweiterung folgen, gelangen Sie zu einer Liste der Dateierweiterungen, die in diesem Fall untersucht werden (s. Anhang A.1 auf S. 256).

Hinweis

Es sollte beachtet werden, dass ein Angreifer einen Virus in einer Datei mit der Erweiterung txt an Ihren Computer senden kann, obwohl es sich in Wirklichkeit um eine ausführbare Datei handelt, die in eine txt-Datei umbenannt wurde. Wenn Sie die Variante **Programme und Dokumente (nach Erweiterung) untersuchen** wählen, wird eine solche Datei bei der Untersuchung übersprungen. Wenn Sie die Variante **Programme und Dokumente (nach Inhalt) untersuchen** gewählt haben, analysiert das Programm ungeachtet der Erweiterung die Kopfzeile der Datei, wodurch sich ergibt, dass die Datei das Format exe besitzt. Eine solche Datei wird der sorgfältigen Virusuntersuchung unterzogen.

Im Abschnitt **Optimierung** lässt sich festlegen, dass nur Dateien untersucht werden sollen, die neu sind oder seit ihrer letzten Analyse verändert wurden. Dieser Modus erlaubt es, die Untersuchungszeit wesentlich zu verkürzen und die Arbeitsgeschwindigkeit des Programms zu erhöhen. Aktivieren Sie dazu das Kontrollkästchen **Nur neue und veränderte Dateien untersuchen**. Dieser Modus erstreckt sich auf gewöhnliche und zusammengesetzte Dateien.

Geben Sie im Abschnitt **Zusammengesetzte Dateien** an, welche zusammengesetzten Dateien auf Viren untersucht werden sollen:

Außerdem kann im Abschnitt **Optimierung** eine Begrenzung für die Untersuchungszeit und die maximale Größe eines einzelnen Objekts festgelegt werden.

- **Untersuchung beenden, wenn länger als ... Sek**. Aktivieren Sie das Kontrollkästchen, um die Untersuchung eines einzelnen Objekts in zeitlicher Hinsicht zu begrenzen, und geben Sie die maximale Untersuchungsdauer für ein Objekt im Feld rechts an. Bei einer Überschreitung der Zeitbegrenzung wird das Objekt von der Untersuchung ausgeschlossen.
- **Archive nicht untersuchen, wenn größer als ... MB**. Aktivieren Sie das Kontrollkästchen, um die Untersuchung eines einzelnen Objekts hinsichtlich der Größe zu begrenzen, und geben Sie die maximal zulässige Größe eines Objekts im Feld rechts an. Bei einer Überschreitung der Größenbegrenzung wird das Objekt von der Untersuchung ausgeschlossen.

Geben Sie im Abschnitt **Zusammengesetzte Dateien** an, welche zusammengesetzten Dateien auf Viren analysiert werden sollen:

- **Alle/Nur neue Archive untersuchen** – Archive der Formate RAR, ARJ, ZIP, CAB, LHA, JAR, ICE untersuchen.

Achtung!

Archive, in denen Kaspersky Anti-Virus die Desinfektion nicht unterstützt (z.B. HA, UUE, TAR), werden nicht automatisch gelöscht, selbst wenn als Aktion die automatische Desinfektion oder das Löschen irreparabler Objekte gewählt wurde.

Verwenden den Link Archiv löschen im Meldungsfenster über den Fund des gefährlichen Objekts, um solche Archive zu löschen. Diese Meldung erscheint auf dem Bildschirm, nachdem die Bearbeitung von während der Untersuchung gefundenen Objekten gestartet wurde. Außerdem kann ein infiziertes Archiv auch manuell aus dem Computer entfernt werden.

- **Alle/Nur neue angehängte(n) OLE-Objekte untersuchen** – Objekte, die in eine Datei eingebettet sind, untersuchen (beispielsweise eine Excel-Tabelle oder ein Makro, das in eine Microsoft Word-Datei eingebettet ist, der Anhang einer E-Mail-Nachricht, usw.).

Für jeden Typ einer zusammengesetzten Datei können Sie wählen, ob alle oder nur neue Dateien untersucht werden sollen. Verwenden Sie dazu den Link neben der Bezeichnung des Objekts. Der Link verändert seinen Wert, wenn mit der linken Maustaste darauf geklickt wird. Wenn im Abschnitt **Optimierung** festgelegt wurde, dass nur neue und veränderte Dateien untersucht werden sollen, steht die Auswahl des Typs der zusammengesetzten Dateien nicht zur Verfügung.

Mailformatdateien untersuchen – Dateien in Mailformaten und Mail-Datenbanken untersuchen. Wenn das Kontrollkästchen aktiviert ist, zerlegt Kaspersky Anti-Virus eine Mailformatdatei und analysiert jede Komponente der E-Mail (Briefkörper, Anhang) auf Viren. Wenn das Kontrollkästchen nicht angekreuzt ist, wird die Mailformatdatei als einheitliches Objekt untersucht.

Achtung!
Beachten Sie folgende Besonderheiten bei der Untersuchung von Mail-Datenbanken, die durch Kennwort geschützt sind:

- Kaspersky Anti-Virus erkennt schädlichen Code in Datenbanken für Microsoft Office Outlook 2000, desinfiziert diese aber nicht.
- Das Programm unterstützt die Suche nach schädlichem Code in geschützten Mail-Datenbanken für Microsoft Office Outlook 2003 nicht.

Kennwortgeschützte Archive untersuchen – Untersuchung von Archiven, die durch Kennwort geschützt sind. In diesem Fall erfolgt vor der Untersuchung von Objekten, die in dem Archiv enthalten sind, auf dem Bildschirm eine Kennwortabfrage. Wenn das Kontrollkästchen nicht aktiviert ist, werden kennwortgeschützte Archive bei der Untersuchung übersprungen.

11.4.3. Zusätzliche Optionen für die Virensuche

Neben der Konfiguration der grundlegenden Parameter für die Virenuntersuchung können Sie noch zusätzliche Parameter festlegen (s. Abb. 47):

iChecker-Technologie verwenden – Die Verwendung dieser Technologie erlaubt eine Steigerung der Untersuchungsgeschwindigkeit, weil bestimmte Objekte von der Untersuchung ausgeschlossen werden. Das Ausschließen eines Objekts von der Untersuchung erfolgt nach einem speziellen Algorithmus, der das Erscheinungsdatum der Programm-Datenbanken, das Datum der letzten Untersuchung des Objekts und die Änderung von Untersuchungseinstellungen berücksichtigt.

Wurde beispielsweise eine Archivdatei vom Programm untersucht und ihr wurde der Status virenfrei zugewiesen, dann wird das Archiv von der folgenden Untersuchung ausgeschlossen, wenn es nicht verändert wurde und

die Untersuchungsparameter gleich geblieben sind. Wenn Sie die Zusammensetzung des Archivs durch das Hinzufügen eines neuen Objekts verändert, die Untersuchungsparameter geändert haben, oder wenn die Programm-Datenbanken aktualisiert wurden, wird das Archiv erneut untersucht.

Die Technologie iChecker™ besitzt Einschränkungen: Sie funktioniert nicht mit großen Dateien und kann nur auf Objekte angewandt werden, deren Struktur der Anwendung Kaspersky Anti-Virus bekannt ist (z.B. die Dateiformate *exe*, *dll*, *lnk*, *ttf*, *inf*, *sys*, *com*, *chm*, *zip*, *rar*).

- **iSwift-Technologie verwenden** – Diese Technologie stellt eine Weiterentwicklung der iChecker-Technologie für Computer mit NTSF-Dateisystem dar. Die Technologie iSwift besitzt folgende Einschränkungen: Sie ist an einen konkreten Ort der Datei im Dateisystem gebunden und kann nur auf Objekte angewandt werden, die sich in einem NTFS-Dateisystem befinden.
- **Informationen über gefährliche Objekte in die Programmstatistik eintragen** – Informationen über den Fund gefährlicher Objekte in der Gesamtstatistik des Programms speichern und im Berichtsfenster auf der Registerkarte **Gefunden** eine Liste der gefährlichen Bedrohungen anzeigen (s. Pkt. 15.3.2 auf S. 199). Wenn das Kontrollkästchen deaktiviert wird, werden keine Informationen über gefährliche Objekte im Bericht angezeigt und diese Objekte können folglich auch nicht bearbeitet werden.
- **Ressourcen für andere Anwendungen freigeben** – Die Ausführung dieser Untersuchungsaufgabe anhalten, wenn die Prozessorressourcen von anderen Anwendungen beansprucht werden.

Abbildung 47. Erweiterte Untersuchungseinstellungen

11.4.4. Suche nach Rootkits

Ein Rootkit ist eine Kombination von Utilities, die schädliche Programme im Betriebssystem verstecken. Solche Utilities dringen ins System ein, tarnen ihre Existenz sowie die Existenz von in der Konfiguration des Rootkits beschriebener Malware, die sich in Prozessen, Ordnern oder Registrierungsschlüsseln des Systems befinden kann.

Die Suche nach Rootkits kann mit jeder beliebigen Untersuchungsaufgabe ausgeführt werden (unter der Bedingung, dass diese Option in den Einstellungen der Aufgabe aktiviert wurde). Außerdem haben die Kaspersky-Lab-Spezialisten für die Suche nach schädlichen Programmen dieses Typs eine separate Aufgabe erstellt und optimal angepasst.

Um die Suche nach Rootkits zu aktivieren, setzen Sie im Block **Rootkit-Suche** das Häkchen im Kontrollkästchen ☑ **Rootkit-Suche aktivieren**. Wenn die Rootkit-Suche aktiviert ist, können Sie die Detailstufe für die Suche nach Rootkits einschalten. Aktivieren Sie dazu das Kontrollkästchen ☑ **Erweiterte Rootkit-Suche aktivieren**. In diesem Fall wird die ausführliche Suche nach

solchen Programmen ausgeführt, wobei eine große Anzahl von Objekten unterschiedlicher Typen analysiert wird. In der Grundeinstellung sind die Kontrollkästchen deaktiviert, weil dieser Modus die Systemressourcen relativ stark beansprucht.

Um die Suche nach Rootkits anzupassen:

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie im Abschnitt **Virensuche** den Namen der Aufgabe.
2. Klicken Sie im Block **Sicherheitsstufe** (s. Abb. 45) auf die Schaltfläche **Einstellungen** und gehen Sie im folgenden Fenster auf die Registerkarte **Heuristische Analyse** (s. Abb. 48).

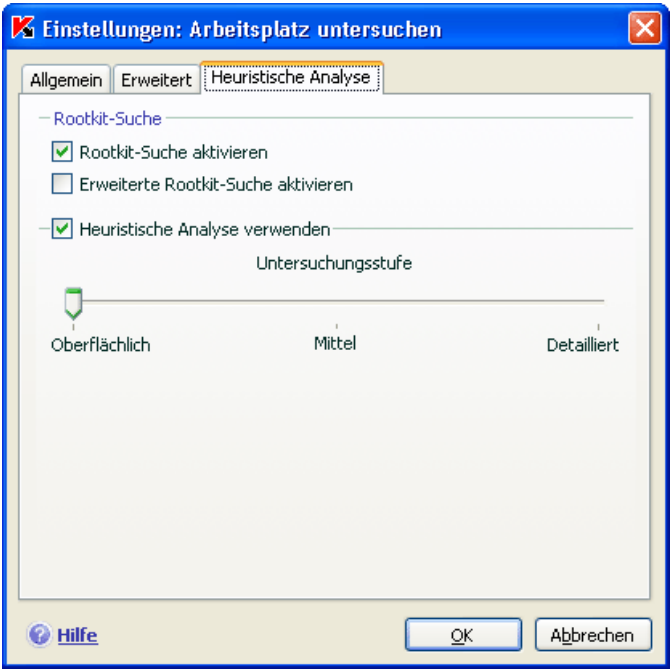


Abbildung 48. Konfiguration der Parameter für Rootkit-Suche und Verwendung heuristischer Methoden

11.4.5. Verwendung heuristischer Analysemethoden

Heuristische Analysemethoden werden bei der Arbeit bestimmter Echtzeitschutz-Komponenten und bei Aufgaben zur Virensuche verwendet (Details s. Pkt. 7.2.4 auf S. 98).

Auf der Registerkarte **Heuristische Analyse** (s. Abb. 48) können Sie die Verwendung von heuristischen Methoden zur Suche neuer Bedrohungen im Rahmen von Untersuchungsaufgaben aktivieren/deaktivieren. Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie im Abschnitt **Virensuche** den Namen der Aufgabe.
2. Klicken Sie im Block **Sicherheitsstufe** auf die Schaltfläche **Einstellungen** und gehen Sie im folgenden Fenster auf die Registerkarte **Heuristische Analyse**.

Um die heuristischen Methoden zu verwenden, aktivieren Sie das Kontrollkästchen **Heuristische Analyse verwenden**. Sie können zusätzlich die Genauigkeitsstufe der Untersuchung anpassen. Bewegen Sie dazu den Schieberegler auf die gewünschte Position: **Oberflächlich**, **Mittel** oder **Detailliert**.

11.4.6. Wiederherstellen der standardmäßigen Untersuchungseinstellungen

Während der Konfiguration der Parameter für die Aufgabenausführung können Sie jederzeit zu den empfohlenen Einstellungen zurückkehren. Diese gelten als optimal, werden von den Kaspersky-Lab-Spezialisten empfohlen und sind in der Sicherheitsstufe **Empfohlen** zusammengefasst.

Um die standardmäßigen Untersuchungseinstellungen für Objekte wiederherzustellen,

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie im Abschnitt **Virensuche** den Aufgabenname.
2. Klicken Sie im Block **Sicherheitsstufe** (s. Abb. 45) auf die Schaltfläche **Grundeinstellung**.

11.4.7. Auswahl der Aktion für Objekte

Wenn sich durch die Virenuntersuchung eines Objekts herausstellt, dass es infiziert oder verdächtig ist, hängen die weiteren Operationen des Programms vom Status des Objekts und von der ausgewählten Aktion ab.

Ein Objekt kann aufgrund der Untersuchung einen der folgenden Status erhalten:

- Status eines der schädlichen Programme (beispielsweise *Virus*, *trojanisches Programm*).
- *möglicherweise infiziert*, wenn sich aufgrund der Untersuchung nicht eindeutig feststellen lässt, ob das Objekt infiziert ist oder nicht. Möglicherweise wurde in der Datei die Codefolge eines unbekannten Virus oder der modifizierte Code eines bekannten Virus gefunden.

Standardmäßig werden alle infizierten Dateien der Desinfektion unterzogen und alle möglicherweise infizierten Dateien in die Quarantäne verschoben.

Um die Aktion für ein Objekt zu ändern,

öffnen Sie das Konfigurationsfenster des Programms und wählen Sie im Abschnitt **Virensuche** den Namen der Aufgabe. Alle verfügbaren Aktionen werden im entsprechenden Abschnitt genannt (s. Abb. 49).

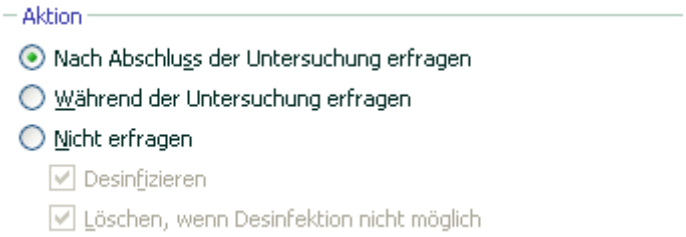


Abbildung 49. Auswahl der Aktion für ein gefährliches Objekt

Gewählte Aktion	Was geschieht beim Fund eines infizierten/ möglicherweise infizierten Objekts?
Nach Abschluss der Untersuchung erfragen	Das Programm schiebt die Bearbeitung von Objekten bis zum Ende der Untersuchung auf. Nach dem Abschluss der Untersuchung erscheint auf dem Bildschirm ein Statistik-Fenster mit einer Liste der gefundenen Objekte und Ihnen wird angeboten, die Objektbearbeitung durchzuführen.
Während der Untersuchung erfragen	Das Programm zeigt eine Warnmeldung auf dem Bildschirm an, die Informationen darüber enthält, von welchem schädlichen Code das Objekt infiziert/möglicherweise infiziert ist, und bietet Aktionen zur Auswahl an.
Nicht erfragen	Das Programm protokolliert im Bericht Informationen über die gefundenen Objekte. Die Objekte werden nicht bearbeitet und der Benutzer wird nicht benachrichtigt. Es wird davor gewarnt, diesen Funktionsmodus für das Programm zu wählen, weil infizierte und möglicherweise infizierte Objekte dann auf Ihrem Computer verbleiben und es praktisch unmöglich ist, eine Infektion zu verhindern.

Gewählte Aktion	Was geschieht beim Fund eines infizierten/ möglicherweise infizierten Objekts?
Nicht erfragen **Desinfizieren**	Das Programm führt einen Desinfektionsversuch mit dem gefundenen Objekt aus, ohne nach der Bestätigung des Benutzers zu fragen. Wenn der Desinfektionsversuch erfolglos bleibt, erhält das Objekt den Status *cherweise infiziert* und wird in die Quarantäne verschoben (s. Pkt. 15.1 auf S. 188). Informationen darüber werden im Bericht aufgezeichnet (s. Pkt. 15.3 auf S. 195). Später kann versucht werden, das Objekt zu desinfizieren.
Nicht erfragen **Desinfizieren** **Löschen, wenn Desinfektion nicht möglich**	Das Programm führt einen Desinfektionsversuch mit dem gefundenen Objekt aus, ohne nach der Bestätigung des Benutzers zu fragen. Wenn der Desinfektionsversuch erfolglos bleibt, wird das Objekt gelöscht.
Nicht erfragen **Desinfizieren** **Löschen**	Das Programm löscht das Objekt automatisch.

Bevor ein Desinfektionsversuch erfolgt oder das Objekt gelöscht wird, legt Kaspersky Anti-Virus eine Sicherungskopie des Objekts an und speichert diese im Backup (s. Pkt. 15.2 auf S. 193). Dadurch wird es möglich, das Objekt bei Bedarf wiederherzustellen oder möglicherweise später zu desinfizieren.

11.4.8. Festlegen einheitlicher Untersuchungsparameter für alle Aufgaben

Jede Untersuchungsaufgabe wird mit eigenen Parametern ausgeführt. Für die Aufgaben, die bei der Programminstallation auf dem Computer erstellt wurden,

gelten standardmäßig die von den Kaspersky-Lab-Spezialisten empfohlenen Parameter.

Sie können einheitliche Untersuchungsparameter für alle Aufgaben festlegen. Als Grundlage gilt dabei die Auswahl der Parameter, die bei der Virenuntersuchung eines einzelnen Objekts verwendet werden.

Um einheitliche Untersuchungsparameter für alle Aufgaben festzulegen:

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie den Abschnitt **Virensuche**.
2. Legen Sie folgende Untersuchungsparameter fest: Wählen Sie die Sicherheitsstufe (s. Pkt. 11.4.1 auf S. 156), nehmen Sie die erweiterten Einstellungen für die Sicherheitsstufe vor und bestimmen Sie die Aktion für Objekte (s. Pkt. 11.4.7 auf S. 165).
3. Klicken Sie im Block **Einstellungen anderer Aufgaben** auf die Schaltfläche **Übernehmen**, um die vorgenommenen Änderungen für alle Aufgaben zu übernehmen. Bestätigen Sie das Festlegen der einheitlichen Parameter.

KAPITEL 12. TESTEN DER ARBEIT VON KASPERSKY ANTI-VIRUS

Nach Installation und Konfiguration von Kaspersky Anti-Virus wird empfohlen, die Korrektheit von Einstellungen und Funktion der Anwendung mit Hilfe eines "Testvirus" und seinen Modifikationen zu prüfen.

12.1. EICAR-"Testvirus" und seine Modifikationen

Dieser Testvirus wurde vom Institut eicar (The European Institute for Computer Antivirus Research) speziell zum Überprüfen der Arbeit von Antiviren-Produkten entwickelt.

Der "Testvirus" IST KEIN VIRUS und enthält keinen Programmcode, der Ihren Rechner beschädigen könnte. Trotzdem wird er von den meisten Antiviren-Softwareprodukten als Virus erkannt.

> **Achtung!**
>
> Verwenden Sie nie echte Viren, um die Funktionsfähigkeit eines Antiviren-Produkts zu testen!

Der "Testvirus" kann von der offiziellen Internetseite des **EICAR**-Instituts heruntergeladen werden: http://www.eicar.org/anti_virus_test_file.htm.

Die von der Webseite des **EICAR**-Instituts heruntergeladene Datei enthält den Code des standardmäßigen "Testvirus". Kaspersky Anti-Virus erkennt diese Datei, weist ihr den Typ **Virus** zu und führt die für diesen Objekttyp festgelegte Aktion aus.

Um die Reaktion von Kaspersky Anti-Virus beim Fund von Objekten eines anderen Typs zu prüfen, können Sie den Inhalt des standardmäßigen "Testvirus" durch Hinzufügen eines Präfixes modifizieren (s. Tabelle).

Präfix	Status des "Testvirus"	Entsprechende Aktion bei der Bearbeitung des Objekts durch die Anwendung
kein Präfix, standard-mäßiger "Testvirus"	Die Datei enthält den "Testvirus". Die Desinfektion ist nicht möglich.	Die Anwendung identifiziert dieses Objekt als schädlich und irreparabel. Das Objekt wird gelöscht.
CORR-	Beschädigt.	Die Anwendung hat Zugriff auf das Objekt erhalten, kann es aber nicht untersuchen, weil es beschädigt ist (z.B. Struktur des Objekts ist beschädigt, ungültiges Dateiformat).
SUSP- WARN-	Die Datei enthält den "Testvirus" (Modifikation). Die Desinfektion ist nicht möglich.	Dieses Objekt ist eine Modifikation eines bekannten Virus oder ein unbekannter Virus. Im Moment des Funds enthalten die Datenbanken mit den Programm-Datenbanken keine Beschreibung zur Desinfektion dieses Objekts. Die Anwendung verschiebt das Objekt in die Quarantäne, um es später mit aktualisierten Datenbanken zu bearbeiten.
ERRO-	Bearbeitungsfehler.	Während der Bearbeitung des Objekts ist ein Fehler aufgetreten: Die Anwendung erhält keinen Zugriff auf das Untersuchungs-objekt, weil die Integrität des Objekts beschädigt ist (z.B. kein Endpunkt in einem Multi-Level-Archiv) oder die Verbindung zu dem Objekt fehlt (wenn ein Objekt in einer Netzwerkressource untersucht wird).
CURE-	Die Datei enthält den "Testvirus". Die Desinfektion ist möglich. Das Objekt kann repariert	Das Objekt enthält einen Virus, der desinfiziert werden kann. Die Anwendung führt die Antiviren-Bearbeitung des Objekts durch.

Präfix	Status des "Testvirus"	Entsprechende Aktion bei der Bearbeitung des Objekts durch die Anwendung
	werden, wobei der Text des "Viruskörpers" in `CURE` geändert wird.	Danach ist das Objekt vollständig repariert.
`DELE-`	Die Datei enthält den "Testvirus". Die Desinfektion ist nicht möglich.	Dieses Objekt ist irreparabel von einem Virus infiziert oder ist ein trojanisches Programm. Die Anwendung löscht solche Objekte.

Die erste Spalte der Tabelle enthält Präfixe, die dem standardmäßigen "Testvirus" am Zeilenanfang hinzugefügt werden können. In der zweiten Spalte werden für die unterschiedlichen Typen des "Testvirus" der Status und die Reaktion von Kaspersky Anti-Virus beschrieben. Die dritte Spalte bietet Informationen über die vom Status abhängige Bearbeitung der Objekte durch die Anwendung.

Die Aktionen für das jeweilige Objekt werden durch die vorgegebenen Einstellungen für die Antiviren-Untersuchung festgelegt.

12.2. Testen des Datei-Anti-Virus

Um die Funktionsfähigkeit von Datei-Anti-Virus zu testen:

1. Erlauben Sie das Protokollieren aller Ereignisse im Bericht, damit Daten über beschädigte Objekte oder Objekte, die aufgrund einer Störung nicht untersucht werden, in der Berichtsdatei gespeichert werden. Aktivieren Sie dazu im Konfigurationsfenster des Programms im Abschnitt **Datenverwaltung** das Kontrollkästchen ☑ **Informative Ereignisse protokollieren** (s. Pkt. 15.3.1 auf S. 198).
2. Erstellen Sie einen Ordner auf der Festplatte. Kopieren Sie den von der offiziellen EICAR-Seite (s. Pkt. 12.1 auf S. 169) heruntergeladenen "Testvirus" und die von Ihnen erstellten Modifikationen des "Testvirus" in diesen Ordner.

Datei-Anti-Virus fängt den Zugriff auf die Datei ab, untersucht sie und benachrichtigt Sie über den Fund eines gefährlichen Objekts:

Abbildung 50. Ein gefährliches Objekt wurde gefunden

Durch die Auswahl unterschiedlicher Aktionsvarianten für ein gefundenes Objekt können Sie die Reaktion von Datei-Anti-Virus auf den Fund verschiedener Objekttypen testen.

Das vollständige Arbeitsergebnis von Datei-Anti-Virus ist im Bericht über die Arbeit der Komponente enthalten.

12.3. Testen einer Aufgabe zur Virensuche

Um eine Untersuchungsaufgabe zu testen:

1. Erstellen Sie einen Ordner auf der Festplatte. Kopieren Sie den von der offiziellen EICAR-Seite (s. Pkt. 12.1 auf S. 169) heruntergeladenen "Testvirus" und die von Ihnen erstellten Modifikationen des "Testvirus" in diesen Ordner.
2. Erstellen Sie eine neue Aufgabe (s. Pkt. 11.3 auf S. 153) zur Virensuche und wählen Sie als Untersuchungsobjekt den Ordner (s. Pkt. 11.2 auf S. 152), der die "Testviren" enthält.

3. Erlauben Sie das Protokollieren aller Ereignisse, damit Daten über beschädigte Objekte oder Objekte, die aufgrund einer Störung nicht untersucht wurden, in der Berichtsdatei gespeichert werden. Aktivieren Sie dazu im Konfigurationsfenster des Programms im Abschnitt **Datenverwaltung** das Kontrollkästchen ☑ **Informative Ereignisse protokollieren** (s. Pkt. 15.3.1 auf S. 198).

4. Starten Sie die Ausführung der Aufgabe zur Virensuche (s. Pkt. 11.1 auf S. 151).

Während der Untersuchung werden beim Fund verdächtiger oder infizierter Objekte auf dem Bildschirm Meldungen mit Informationen über das Objekt und einer Bestätigungsabfrage zur folgenden Aktion angezeigt:

Abbildung 51. Ein gefährliches Objekt wurde gefunden

Durch die Auswahl unterschiedlicher Aktionsvarianten können Sie die Reaktion von Kaspersky Anti-Virus auf den Fund der einzelnen Objekttypen testen.

Das vollständige Arbeitsergebnis der Ausführung der Untersuchungsaufgabe ist im Bericht über die Arbeit der Komponente enthalten.

KAPITEL 13. UPDATE DES PROGRAMMS

Eine Voraussetzung für die Sicherheit Ihres Computers ist die Pflege des aktuellen Zustands von Kaspersky Anti-Virus. Jeden Tag tauchen neue Viren, Trojaner und andere schädliche Programme auf. Deshalb ist es sehr wichtig sicherzustellen, dass Ihre Informationen zuverlässig geschützt werden.

Die Aktualisierung des Programms umfasst den Download und die Installation folgender Elemente auf Ihren Computer:

Anti-Virus-Datenbanken und Netzwerktreiber

Der Schutz der Informationen auf ihrem Computer basiert auf den Signaturen der Bedrohungen. Die Schutzkomponenten verwenden diese bei der Suche und Desinfektion gefährlicher Objekte auf Ihrem Computer. Die Datenbanken werden stündlich durch Einträge über neue Bedrohungen und entsprechende Desinfektionsmethoden ergänzt. Deshalb wird ausdrücklich empfohlen, die Datenbanken regelmäßig zu aktualisieren.

Gemeinsam mit den Anti-Virus-Datenbanken werden auch die Netzwerktreiber aktualisiert, die die Funktionalität für das Abfangen des Netzwerkverkehrs durch die Schutzkomponenten gewährleisten.

In den vorhergehenden Versionen der Antiviren-Anwendungen von Kaspersky Lab wurde die Arbeit mit unterschiedlichen Typen von Datenbanken unterstützt: *Standard-* oder *erweiterte Auswahl*. Sie unterschieden sich im Hinblick auf die Typen der gefährlichen Objekte, vor denen Sie Ihren Computer schützten. In Kaspersky Anti-Virus 7.0 brauchen Sie sich nicht um die Auswahl des passenden Typs der Datenbanken kümmern. Bei der Arbeit unserer Produkte werden jetzt Programm-Datenbanken verwendet, die den Schutz vor unterschiedlichen Arten schädlicher und potentiell gefährlicher Objekte bieten.

Programm-Module

Neben den Programm-Datenbanken können Sie auch die internen Module von Kaspersky Anti-Virus aktualisieren. Kaspersky Lab gibt periodisch Updatepakete heraus.

Als primäre Updatequelle für Kaspersky Anti-Virus gelten die speziellen Kaspersky-Lab-Updateserver. Für den erfolgreichen Updatedownload von den Servern ist eine Verbindung Ihres Computers mit dem Internet erforderlich.

Hinweis

Für den erfolgreichen Updatedownload von den Servern ist eine Verbindung Ihres Computers mit dem Internet erforderlich. Wenn die Internetverbindung über einen Proxyserver erfolgt, ist es erforderlich, die entsprechenden Verbindungsparameter anzupassen (s. Pkt. 15.7 auf S. 213).

Wenn Sie keinen Zugriff auf die Kaspersky-Lab-Updateserver besitzen (wenn beispielsweise kein Internetzugang vorhanden ist), können Sie unter folgenden Nummern unsere Hauptverwaltung anrufen: +7 (495) 797 87 00, +7 (495) 645 79 39, +7 (495) 956 70 00 oder +7 (495) 956-00-00. Dort können Sie die Adressen der Partner von Kaspersky Lab erfahren, die Ihnen die Updates auf Disketten oder CDs/DVDs im zip-Format anbieten können.

Der Updatedownload erfolgt in einem der folgenden Modi:

- *Automatisch*. Kaspersky Anti-Virus prüft in festgelegten Zeitabständen, ob an der Updatequelle ein neues Updatepaket vorhanden ist. Die Häufigkeit der Überprüfung kann während Virusepidemien steigen und unter gewöhnlichen Umständen sinken. Wenn neue Updates vorhanden sind, lädt die Anwendung sie herunter und installiert sie auf dem Computer. Dieser Modus gilt als Standard.
- *Nach Zeitplan*. Die Aktualisierung des Programms erfolgt nach einem festgelegten Zeitplan.
- *Manuell*. In diesem Fall starten Sie die Aktualisierung des Programms selbständig.

Beim Updatevorgang werden die Programm-Module und die Datenbanken auf Ihrem Computer mit den auf der Updatequelle vorhandenen verglichen. Wenn auf Ihrem Computer die aktuelle Version der Datenbanken und Module installiert ist, erscheint auf dem Bildschirm eine Meldung über die Aktualität des Schutzes auf Ihrem Computer. Wenn Datenbanken und Module nicht aktuell sind, wird nur der fehlende Teil der Updates auf Ihrem Computer installiert. Datenbanken und Module werden nicht vollständig kopiert, wodurch die Updategeschwindigkeit wesentlich gesteigert und der Netzwerkverkehr entlastet wird.

Bevor die Programm-Datenbanken aktualisiert werden, legt Kaspersky Anti-Virus eine Sicherungskopie davon an. Bei Bedarf können Sie zu den vorhergehenden Datenbanken zurückkehren.

Die Möglichkeit des Rollbacks (s. Pkt. 13.2 auf S. 176) ist beispielsweise erforderlich, wenn Sie die Datenbanken aktualisiert haben und diese bei der Arbeit beschädigt wurden. Sie können zu der vorhergehenden Variante der Datenbanken zurückkehren und ihre Aktualisierung später erneut versuchen.

Während die Anwendung aktualisiert wird, können Sie gleichzeitig die Verteilung der heruntergeladenen Updates in eine lokale Quelle ausführen (s. Pkt. 13.3.3

auf S. 182). Dieser Dienst erlaubt es, die Datenbanken und Module, die von Anwendungen der Version 7.0 verwendet werden, auf den Netzwerkcomputern zu aktualisieren und dadurch Netzwerkverkehr einzusparen.

13.1. Starten des Updates

Sie können das Programm-Update jederzeit starten. Die Aktualisierung erfolgt von der von Ihnen gewählten Updatequelle (s. Pkt. 13.3.1 auf S. 177).

Das Programm-Update kann gestartet werden:

- aus dem Kontextmenü (s. Pkt. 4.2 auf S. 46).
- aus dem Hauptfenster des Programms (s. Pkt. 4.3 auf S. 48).

Um das Programm-Update aus dem Kontextmenü zu starten,

1. Öffnen Sie das Menü durch Rechtsklick auf das Programmsymbol im Infobereich der Taskleiste von Microsoft Windows.
2. Wählen Sie den Punkt **Update**.

Um das Update aus dem Programmhauptfenster zu starten,

1. Wählen Sie auf der linken Seite des Hauptfensters die Komponente **Update**.
2. Klicken Sie auf den Link Datenbanken aktualisieren

Im Hauptfenster werden Informationen über den Verlauf des Updates angezeigt. Verwenden Sie den Link Details, um den Bericht über die Update-Aufgabe mit ausführlichen Informationen über den Aktualisierungsvorgang zu öffnen. Durch Klick auf die Schaltfläche **Schließen**, können Sie das Berichtsfenster ausblenden, wobei der Updatevorgang fortgesetzt wird.

Hinweis

Beachten Sie, dass beim Ausführen des Updates gleichzeitig die Update-Verteilung in eine lokale Quelle erfolgt, falls dieser Dienst aktiviert wurde (s. Pkt. 13.3.3 auf S. 182).

13.2. Rollback zum vorherigen Update

Jedes Mal, wenn Sie das Programm-Update starten, erstellt Kaspersky Anti-Virus zuerst eine Sicherungskopie der bisher verwendeten Datenbanken und

Programm-Module und geht erst danach zu deren Update über. Dadurch wird Ihnen erlaubt, zur Verwendung der vorhergehenden Version der Datenbanken zurückzukehren, wenn das Update erfolglos war.

Um zur Verwendung der vorhergehenden Version der Datenbanken zurückzukehren,

1. Wählen Sie auf der linken Seite des Programmhauptfensters die Komponente **Update**.
2. Klicken Sie auf der rechten Seite des Hauptfensters auf den Link Rollback zu den vorigen Datenbanken.

13.3. Update-Einstellungen

Das Programm-Update wird genau nach den Parametern ausgeführt, die festlegen:

- von welcher Ressource der Download und die Installation der Programm-Updates erfolgt (s. Pkt. 13.3.1 auf S. 177).
- in welchem Modus die Programmaktualisierung gestartet wird und welche Elemente aktualisiert werden sollen (s. Pkt. 13.3.2 auf S. 180).
- wie oft das Update gestartet werden soll, wenn der Start nach Zeitplan aktiviert ist (s. Pkt. 6.7 auf S. 71).
- unter welchem Benutzerkonto das Update ausgeführt wird (s. Pkt. 6.6 auf S. 70).
- ob die heruntergeladenen Updates in einen lokalen Ordner kopiert werden sollen (s. Pkt. 13.3.3 auf S. 182).
- welche Aktionen nach dem Programm-Update ausgeführt werden sollen (s. Pkt. 13.3.4 auf S. 184).

In diesem Abschnitt des Handbuchs werden alle oben genannten Aspekte ausführlich beschrieben.

13.3.1. Auswahl der Updatequelle

Eine *Updatequelle* ist eine bestimmte Ressource, die Updates der Datenbanken und der internen Module für Kaspersky Anti-Virus enthält. Als Updatequelle können http- oder ftp-Server, lokale oder Netzwerkordner dienen.

Als primäre Quelle für die Aktualisierung dienen die *Updateserver von Kaspersky Lab*. Das sind spezielle Internetseiten, auf denen die Updates der Datenbanken

und der internen Module für alle Kaspersky-Lab-Produkte zur Verfügung gestellt werden.

Wenn Sie keinen Zugriff auf die Kaspersky-Lab-Updateserver besitzen (wenn beispielsweise kein Internetzugang vorhanden ist), können Sie unter folgenden Nummern unsere Hauptverwaltung anrufen: +7 (495) 797 87 00, +7 (495) 645 79 39, +7 (495) 956 70 00 oder +7 (495) 956-00-00. Dort können Sie die Adressen der Partner von Kaspersky Lab erfahren, die Ihnen die Updates auf Disketten oder CDs/DVDs im zip-Format anbieten können.

Achtung!

Geben Sie bei der Bestellung von Updates auf Wechseldatenträgern unbedingt an, ob Sie Updates der internen Anwendungsmodule erhalten möchten.

Die auf einem Wechseldatenträger erhaltenen Updates können Sie auf einer ftp- oder http-Seite oder in einem lokalen oder Netzwerkordner speichern.

Die Auswahl der Updatequelle erfolgt auf der Registerkarte **Updatequelle-Einstellungen** (s. Abb. 52).

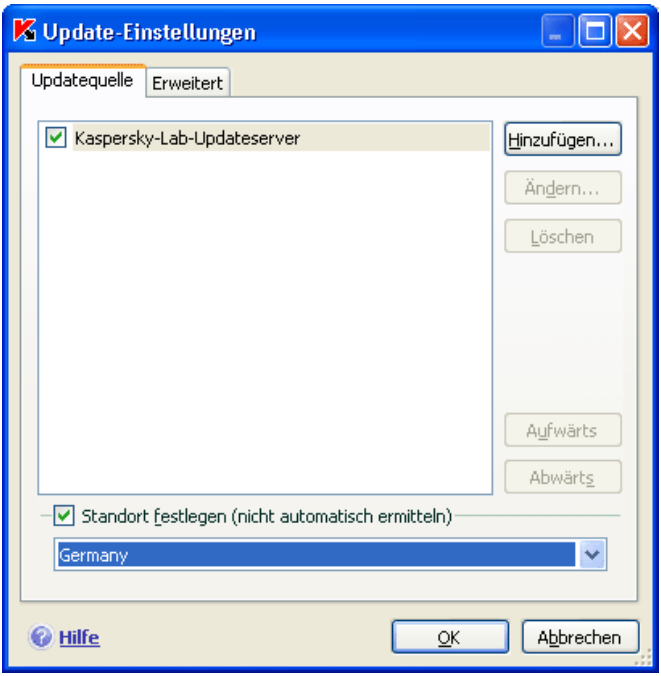


Abbildung 52. Auswahl der Updatequelle

Die Liste enthält standardmäßig nur die Kaspersky-Lab-Updateserver. Die Serverliste kann nicht verändert werden. Beim Updateprozess greift Kaspersky Anti-Virus auf diese Liste zu, wählt die erste Serveradresse aus und versucht, die Updates von dort herunterzuladen. Wenn die Aktualisierung von der gewählten Adresse erfolglos ist, wendet sich das Programm an die nächste Adresse und versucht erneut, die Updates zu empfangen.

Damit die Aktualisierung von einer bestimmten ftp- oder http-Seite erfolgt,

1. klicken Sie auf die Schaltfläche **Hinzufügen**.
2. wählen Sie die http- oder ftp-Seite im Fenster **Updatequelle wählen** oder geben Sie ihre IP-Adresse, ihren symbolischen Namen oder die URL-Adresse im Feld **Quelle** an. Wenn eine ftp-Ressource als Updatequelle gewählt wird, können in der URL-Adresse des Servers die Autorisierungsparameter im Format ftp://user:password@server angegeben werden.

Achtung!

Wenn Sie als Updatequelle eine Ressource gewählt haben, die sich außerhalb des lokalen Netzwerks befindet, ist für die Aktualisierung eine Internetverbindung erforderlich.

Um das Programm aus einem bestimmten Ordner zu aktualisieren,

1. klicken Sie auf die Schaltfläche **Hinzufügen**.
2. wählen Sie den Ordner im Fenster **Updatequelle wählen** oder geben Sie den vollständigen Pfad des Ordners im Feld **Quelle** an.

Kaspersky Anti-Virus fügt die neue Updatequelle am Anfang der Liste hinzu und aktiviert sie automatisch zur Verwendung (aktiviert das entsprechende Kontrollkästchen).

Wenn als Updatequellen mehrere Ressourcen gewählt wurden, dann greift das Programm bei der Aktualisierung streng nach der Listenreihenfolge darauf zu und aktualisiert sich von der ersten verfügbaren Quelle. Sie können die Anordnung der Quellen in der Liste mit Hilfe der Schaltflächen **Aufwärts**/**Abwärts** ändern.

Die Quellenliste kann mit den Schaltflächen **Hinzufügen**, **Ändern** und **Löschen** bearbeitet werden. Die Kaspersky-Lab-Updateserver stehen als Quellen nicht für Änderungen oder zum Löschen zur Verfügung.

Wenn Sie die Kaspersky-Lab-Server als Updatequelle verwenden, können Sie den für Sie günstigsten Standort des Servers für den Updatedownload auswählen. Kaspersky Lab besitzt Server in mehreren Ländern der Erde. Die Auswahl des geografisch am nächsten gelegenen Kaspersky-Lab-Updateservers kann die Dauer des Updates verkürzen und die Downloadgeschwindigkeit erhöhen.

Um den nächstliegenden Server zu wählen, aktivieren Sie das Kontrollkästchen **Standort festlegen (nicht automatisch ermitteln)** und wählen Sie aus der Dropdown-Liste das Land aus, in dem Sie sich gerade aufhalten. Wenn das Kontrollkästchen aktiviert ist, erfolgt das Update unter Berücksichtigung des in der Liste ausgewählten Standorts. Standardmäßig ist das Kontrollkästchen deaktiviert und beim Update werden Informationen über den aktuellen Standort aus der Registrierung des Betriebssystems verwendet.

13.3.2. Auswahl von Updatemodus und Update-Objekt

Ein wichtiger Faktor bei der Konfiguration des Programm-Updates ist das Festlegen von Update-Objekt und Updatemodus.

Das Update-Objekt (s. Abb. 53) bestimmt, bestimmt, welche Elemente aktualisiert werden:

- Programm-Datenbanken
- Netzwerktreiber, die die Funktionalität für das Abfangen des Netzwerkverkehrs durch die Schutzkomponenten gewährleisten.
- Programm-Module

Programm-Datenbanken und Netzwerktreiber werden immer aktualisiert, die Programm-Module nur dann, wenn der entsprechende Modus aktiviert ist..

Abbildung 53. Auswahl des Update-Objekts

Damit beim Updateprozess die Updates der Programm-Module auf Ihren Computer kopiert und installiert werden,

öffnen Sie das Konfigurationsfenster des Programms, wählen Sie den Abschnitt **Update** und aktivieren Sie das Kontrollkästchen **Programm-Module aktualisieren**

Wenn im Augenblick in der Quelle ein Update für die Programm-Module vorhanden ist, lädt das Programm die erforderlichen Updates herunter und installiert sie nach dem Neustart des Computers. Die heruntergeladenen Updates für die Module werden nicht vor dem Neustart installiert.

Erfolgt das nächste Update vor dem Neustart des Computers und der Installation der bereits heruntergeladenen Updates für die Programm-Module, dann werden nur die Programm-Datenbanken aktualisiert.

Der Updatemodus (s. Abb. 54) bestimmt, auf welche Weise die Aktualisierung gestartet wird. Sie können im Block **Startmodus** einen der folgenden Modi wählen:

- **Automatisch**. Kaspersky Anti-Virus prüft in festgelegten Zeitabständen, ob an der Updatequelle (s. Pkt. 13.3.1 auf S. 177) ein neues Updatepaket vorhanden ist. Wenn neue Updates vorliegen, lädt Kaspersky Anti-Virus sie herunter und installiert sie auf dem Computer. Dieser Updatemodus wird standardmäßig benutzt.

  Wenn als Quelle eine Netzwerkressource gewählt wurde, führt Kaspersky Anti-Virus in dem Intervall, das im vorhergehenden Updatepaket angegeben ist, einen Updateversuch durch. Aus einer lokalen Quelle erfolgt das Update im Intervall, das im vorhergehenden Updatepaket angeben ist. Diese Option erlaubt es, die Updatefrequenz bei Virenepidemien und anderen gefährlichen Situationen automatisch zu regulieren. Das Programm wird rechtzeitig mit aktuellen Updates der Datenbanken und Programm-Module versorgt, was die Möglichkeit des Eindringens gefährlicher Programme auf Ihren Computer verhindert.

Abbildung 54. Auswahl des Startmodus für das Update

- **Nach Zeitplan**. Die Aktualisierung des Programms erfolgt nach einem festgelegten Zeitplan. Wenn Sie zu diesem Updatemodus wechseln möchten, wird Ihnen standardmäßig angeboten, das Update einmal täglich vorzunehmen. Um den Zeitplan anzupassen, klicken Sie auf die Schaltfläche **Ändern** neben der Bezeichnung des Modus und nehmen Sie im folgenden Fenster entsprechende Änderungen vor (Details s. Pkt. 6.7 auf S. 6.7).
- **Manuell**. In diesem Fall starten Sie die Aktualisierung des Programms selbständig. Kaspersky Anti-Virus informiert Sie bei Bedarf über die Notwendigkeit der Aktualisierung:

13.3.3. Update-Verteilung

Wenn PCs zu einem lokalen Netzwerk zusammengeschlossen sind, ist es überflüssig die Updates für jeden Computer einzeln herunterzuladen und zu installieren, weil dadurch eine erhöhte Netzwerkbelastung verursacht wird. Sie können den Dienst zur Update-Verteilung verwenden, der es erlaubt, die Netzwerkbelastung zu senken, indem das Updateverfahren folgendermaßen organisiert wird:

1. Ein Computer des Netzwerks lädt das Paket mit den Updates für die Anwendung von den Kaspersky-Lab-Webservern im Internet oder von einer anderen Webressource, auf der sich die aktuellen Updates befinden, herunter. Die heruntergeladenen Updates werden in einem gemeinsamen Ordner abgelegt.
2. Die übrigen Netzwerkcomputer verwenden den gemeinsamen Ordner zum Download der Updates für die Anwendung.

Um den Dienst zur Update-Verteilung zu aktivieren, kreuzen Sie auf der Registerkarte **Erweitert** (s. Abb. 55) das Kontrollkästchen ☑ **Zielordner für Update-Verteilung** an und geben Sie im darunter liegenden Feld den Pfad des gemeinsamen Ordners an, in dem die heruntergeladenen Updates abgelegt werden. Der Pfad kann manuell eingegeben oder im Fenster, das mit der Schaltfläche **Durchsuchen** geöffnet wird, gewählt werden. Wenn das Kontrollkästchen aktiviert ist, werden neue Updates beim Download automatisch in diesen Ordner kopiert.

Achtung!

Beachten Sie, dass Kaspersky Anti-Virus 7.0 von den Kaspersky-Lab-Updateservern nur das Updatepaket für die Anwendungen der Version 7.0 erhält.

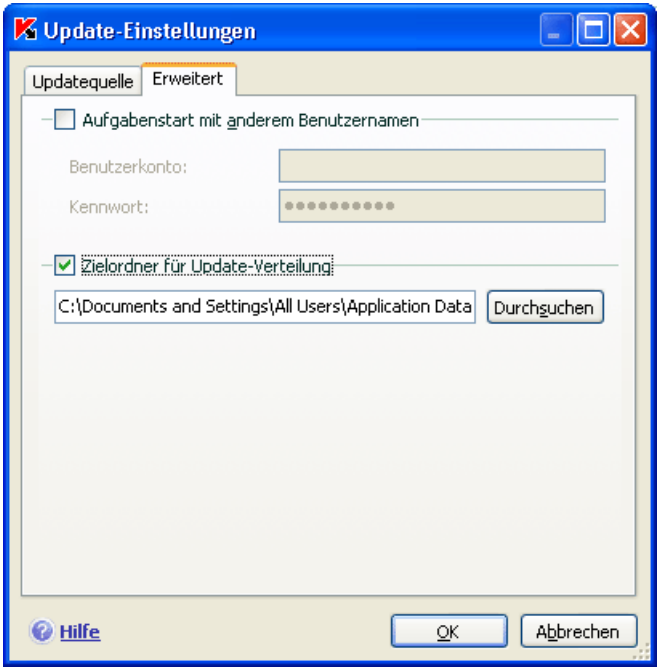


Abbildung 55. Einstellungen für den Dienst zur Update-Verteilung

Damit die anderen Netzwerkcomputer aus dem Ordner aktualisiert werden, der die aus dem Internet kopierten Updates enthält, sind folgende Einstellungen erforderlich.

1. Der gemeinsame Zugriff auf diesen Ordner muss gewährt werden.
2. Der gemeinsame Ordner muss in den Update-Einstellungen der Netzwerkcomputer als Updatequelle angegeben werden.

13.3.4. Aktionen nach dem Programm-Update

Jedes Update der Programm-Datenbanken enthält neue Einträge, die es erlauben, Ihren Computer vor neu aufgetauchten Bedrohungen zu schützen.

Die Kaspersky-Lab-Spezialisten empfehlen Ihnen, sofort nach dem Programm-Update die *in der Quarantäne gespeicherten Objekte* und die *Autostart-Objekte* zu untersuchen.

Warum gerade diese Objekte?

In die Quarantäne werden Objekte verschoben, bei deren Untersuchung nicht genau festgestellt werden konnte, von welchen schädlichen Programmen sie infiziert sind (s. Pkt. 15.1 auf S. 188). Möglicherweise kann Kaspersky Anti-Virus die Gefahr eindeutig bestimmen und desinfizieren, nachdem die Datenbanken aktualisiert wurden.

Das Programm untersucht die Quarantäneobjekte standardmäßig nach jedem Update. Es wird empfohlen, die Objekte in der Quarantäne regelmäßig zu überprüfen. Aufgrund der Untersuchung kann sich der Status einzelner Objekte ändern. Bestimmte Objekte können am ursprünglichen Ort wiederhergestellt und wieder verwendet werden.

Damit keine Untersuchung der Quarantäneobjekte erfolgt, deaktivieren Sie das Kontrollkästchen ☑ **Quarantänedateien untersuchen** im Block **Aktion nach dem Update**.

Die Autostart-Objekte gelten hinsichtlich der Sicherheit Ihres Computers als kritischer Bereich. Wenn dieser Bereich von einem Schadprogramm infiziert wird, ist vielleicht sogar der Start des Betriebssystems nicht mehr möglich. Zur Untersuchung dieses Bereichs verfügt Kaspersky Anti-Virus über eine vordefinierte Aufgabe zur Untersuchung der Autostart-Objekte (s. Kapitel 11 auf S. 150). Es wird empfohlen, den Zeitplan dieser Aufgabe so festzulegen, dass sie jedes Mal nach dem Update der Datenbanken automatisch gestartet wird (s. Pkt. 6.7 auf S. 71).

KAPITEL 14. SCHLÜSSEL-VERWALTUNG

Die Möglichkeit zur Nutzung von Kaspersky Anti-Virus wird durch das Vorhandensein einer *Schlüsseldatei* bestimmt. Den Schlüssel erhalten Sie durch den Kauf des Produkts und er berechtigt Sie ab dem Tag der Installation des Schlüssels zur Nutzung der Anwendung.

Ist kein Schlüssel vorhanden und die Anwendung wurde nicht als Testversion aktiviert, dann funktioniert Kaspersky Anti-Virus im Modus, in dem nur ein einziges Update möglich ist. Danach können keine weiteren Aktualisierungen vorgenommen werden.

Wenn eine Testversion der Anwendung aktiviert wurde, stellt Kaspersky Anti-Virus nach Ablauf der Testdauer seine Funktion ein.

Mit Ablauf der Gültigkeitsdauer eines kommerziellen Schlüssels bleibt die Funktionalität des Programms unter Ausnahme der Updatemöglichkeit für die Programm-Datenbanken erhalten. Sie können Ihren Computer mit Hilfe der Untersuchungsaufgaben weiterhin auf das Vorhandensein von Viren untersuchen und die Schutzkomponenten verwenden, allerdings nur mit den Datenbanken, die bei Ablauf der Schlüsselgültigkeit aktuell waren. Demzufolge können wir Ihnen keinen hundertprozentigen Schutz vor neuen Viren garantieren, die nach dem Gültigkeitsende des Schlüssels für das Programm auftreten.

Um eine Infektion Ihres Computers durch neue Viren zu verhindern, empfehlen wird Ihnen, den Schlüssel für die Benutzung des Programms zu verlängern. Kaspersky Anti-Virus benachrichtigt Sie rechtzeitig, wenn die Gültigkeitsdauer des Schlüssels bald abläuft. Es wird bei jedem Programmstart eine entsprechende Meldung auf dem Bildschirm angezeigt.

Informationen zum verwendeten Schlüssel befinden sich im Abschnitt **Aktivierung** des Programmhauptfensters (s. Abb.(s. Abb. 56). Im Block **Installierte Schlüssel** werden Nummer, Typ (kommerziell, Test, für Beta-Test), Gültigkeitsdauer des Schlüssels und Anzahl der bis zum Ablauf verbleibenden Tage genannt. Um zusätzliche Informationen anzuzeigen, verwenden Sie den Link Details über die Schlüssel anzeigen.

Wenn Sie die Bedingungen des Lizenzvertrags für die Nutzung der Anwendung lesen möchten, verwenden Sie den Link Lizenzvertrag anzeigen. Um einen Schlüssel aus der Liste zu entfernen, verwenden Sie den Link Löschen.

Um einen Schlüssel zu kaufen oder um die Gültigkeitsdauer eines Schlüssels zu verlängern:

1. Kaufen Sie einen neuen Schlüssel. Verwenden Sie dazu den Link Neuen Schlüssel kaufen (falls die Anwendung noch nicht aktiviert wurde) oder Gültigkeit des Schlüssels verlängern. Auf unserer automatisch geöffneten Webseite erhalten Sie umfassende Informationen darüber, zu welchen Bedingungen Sie im Kaspersky-Lab-Internet-Shop oder bei einem autorisierten Händler einen Schlüssel kaufen können.

   Beim Kauf über einen Internet-Shop wird Ihnen nach Eingang der Bezahlung per E-Mail an die im Bestellformular angegebene Adresse eine Schlüsseldatei oder ein Aktivierungscode für das Programm zugeschickt.

2. Installieren Sie den Schlüssel. Verwenden Sie dazu den Link Schlüssel installieren im Abschnitt **Aktivierung** des Hauptfensters von Kaspersky Anti-Virus oder den Befehl **Aktivierung** im Kontextmenü der Anwendung. Dadurch wird der Aktivierungsassistent gestartet (s. Pkt. 3.2.2 auf S. 36).

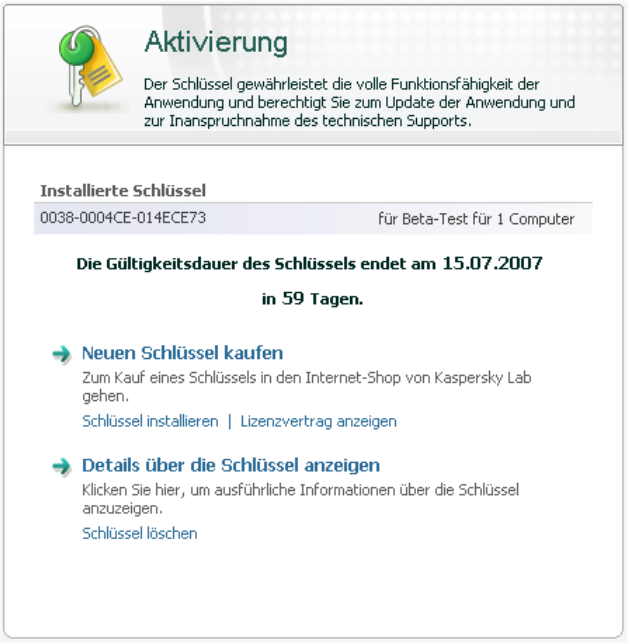

Aktivierung
Der Schlüssel gewährleistet die volle Funktionsfähigkeit der Anwendung und berechtigt Sie zum Update der Anwendung und zur Inanspruchnahme des technischen Supports.
Installierte Schlüssel
0038-0004CE-014ECE73
für Beta-Test für 1 Computer
Die Gültigkeitsdauer des Schlüssels endet am 15.07.2007
in 59 Tagen.
Neuen Schlüssel kaufen
Zum Kauf eines Schlüssels in den Internet-Shop von Kaspersky Lab gehen.
Schlüssel installieren | Lizenzvertrag anzeigen
Details über die Schlüssel anzeigen
Klicken Sie hier, um ausführliche Informationen über die Schlüssel anzuzeigen.
Schlüssel löschen

Abbildung 56. Schlüsselverwaltung

KAPITEL 15. ZUSÄTZLICHE OPTIONEN

Neben dem Schutz Ihrer Daten bietet das Programm zusätzliche Dienste, welche die Funktionalität von Kaspersky Anti-Virus erweitern.

Während der Arbeit verschiebt das Programm bestimmte Objekte in spezielle Speicher. Das Ziel dieses Vorgehens besteht darin, maximalen Datenschutz mit minimalen Verlusten zu gewährleisten.

- Der Backup-Speicher enthält Kopien der Objekte, die aufgrund der Arbeit von Kaspersky Anti-Virus verändert oder gelöscht wurden (s. Pkt. 15.2 auf S. 193). Wenn ein bestimmtes Objekt wichtige Informationen enthielt, die bei der Bearbeitung nicht vollständig erhalten werden konnten, können Sie das Objekt jederzeit über seine Sicherungskopie wiederherstellen.

- Die Quarantäne enthält möglicherweise infizierte Objekte, deren Desinfektion mit der aktuellen Version der Programm-Datenbanken erfolglos war (s. Pkt. 15.1 auf S. 188).

Es wird empfohlen, die Liste der Objekte immer wieder zu überprüfen. Möglicherweise befinden sich veraltete Objekte darunter oder bestimmte Objekte können wiederhergestellt werden.

Folgende Dienste helfen bei der Arbeit mit dem Programm:

- Der Dienst des Technischen Support-Services bietet umfassende Hilfe bei der Arbeit mit Kaspersky Anti-Virus (s. Pkt. 15.10 auf S. 228). Die Experten von Kaspersky Lab haben sich bemüht, alle vorhandenen Unterstützungsmöglichkeiten zu integrieren: Online-Support, Benutzerforum und Wissensdatenbank.

- Der Benachrichtigungsdienst für Ereignisse hilft Ihnen bei der Konfiguration einer Benachrichtigung des Benutzers über wichtige Momente bei der Arbeit von Kaspersky Anti-Virus (s. Pkt. 15.9.1 auf S. 219). Dies können einerseits Ereignisse informativen Charakters sein, andererseits aber Fehler, die unverzüglich behoben werden müssen und hohe Priorität besitzen.

- Der Dienst für den Selbstschutz des Programms und für die Beschränkung des Zugriffs auf die Arbeit mit dem Programm bietet den programmeigenen Dateien Schutz vor Veränderungen und Beschädigungen durch Angreifer, verbietet die externe Steuerung der Programmdienste und kontrolliert die Beschränkung von Rechten anderer Benutzer Ihres Com-

puters zum Ausführen bestimmter Aktionen mit Kaspersky Anti-Virus (s. Pkt. 15.9.2 auf S. 225). Beispielsweise kann das Ändern der Schutzstufe wesentlichen Einfluss auf die Informationssicherheit auf Ihrem Computer ausüben.

- Der Dienst zur Konfigurationsverwaltung erlaubt es, die Funktionsparameter der Anwendung zu speichern und auf andere Computer zu übertragen (s. Pkt. 15.9.3 auf S. 227) sowie die Standardparameter wiederherzustellen (s. Pkt. 15.9.4 auf S. 227).

Darüber hinaus bietet das Programm und detaillierte Berichte (s. Pkt. 15.3 auf S. 195) über die Arbeit aller Schutzkomponenten und die Ausführung aller Aufgaben zur Virensuche und zum Update.

Das Erstellen einer Liste der zu kontrollierenden Ports erlaubt es, die Kontrolle der empfangenen und weitergeleiteten Informationen durch die Schutzkomponenten von Kaspersky Anti-Virus zu regulieren (s. Pkt. 15.5 auf S. 209). Die Konfiguration der Proxyserver-Parameter (s. Pkt. 15.7 auf S. 213) gewährleistet den Zugriff der Anwendung auf das Internet, was für einige Echtzeitschutz-Komponenten und für das Update wichtig ist.

Die Option für das Erstellen einer Notfall-CD zur Systemwiederherstellung erlaubt es, die Funktionsfähigkeit des Computers in dem Zustand wiederherzustellen, der vor einer Infektion herrschte (s. Pkt. 15.4 auf S. 204). Das kann besonders nützlich sein, wenn Systemdateien durch schädlichen Code beschädigt wurden und das Betriebssystem des Computers nicht mehr geladen werden kann.

Außerdem besteht die Möglichkeit, das Aussehen von Kaspersky Anti-Virus zu ändern und die Parameter der aktuellen Programmoberfläche zu konfigurieren (s. Pkt. 15.7 auf S. 213).

Im Folgenden werden alle genannten Dienste ausführlich beschrieben.

15.1. Quarantäne für möglicherweise infizierte Objekte

Die **Quarantäne** ist ein spezieller Speicher, in den Objekte verschoben werden, die möglicherweise von Viren infiziert sind.

Möglicherweise infizierte Objekte sind Objekte, die verdächtig sind, von Viren oder Virenmodifikationen infiziert zu sein.

Warum *möglicherweise infiziert*? Es ist nicht immer möglich, eindeutig festzustellen, ob ein Objekt infiziert ist oder nicht. Dafür gibt es folgende Gründe:

- *Der* Code *des analysierten Objekts besitzt Ähnlichkeit mit einer bekannten Bedrohung, wurde aber teilweise verändert*.

  Die Programm-Datenbanken enthalten jene Bedrohungen, die bisher von den Kaspersky-Lab-Spezialisten untersucht wurden. Wenn ein Schadprogramm verändert wird und diese Veränderungen noch nicht in die Datenbanken aufgenommen wurden, klassifiziert Kaspersky Anti-Virus das Objekt, das von einem veränderten Schadprogramm infiziert ist, als möglicherweise infiziertes Objekt und informiert darüber, welcher Bedrohung diese Infektion ähnelt.

- *Der Code des gefundenen Objekts erinnert an die Struktur eines Schadprogramms. Die Datenbanken enthalten jedoch keine entsprechenden Einträge.*

  Es ist durchaus möglich, dass es sich um eine neue Art von Bedrohung handelt. Deshalb klassifiziert Kaspersky Anti-Virus dieses Objekt als möglicherweise infiziertes Objekt.

Der Verdacht, dass eine Datei durch einen Virus infiziert ist, wird mit dem *heuristischen Code Analysator* ermittelt. Dieser Mechanismus ist sehr effektiv und führt nur selten zu einem Fehlalarm.

Ein verdächtiges Objekt kann während der Virensuche sowie bei der Arbeit von Datei-Anti-Virus, Mail-Anti-Virus und Proaktivem Schutz gefunden und in die Quarantäne verschoben werden.

Sie können eine Datei selbst in die Quarantäne verschieben. Dazu dient der Link Quarantäne in der speziellen Meldung, die beim Fund eines möglicherweise infizierten Objekts auf dem Bildschirm Ihres Computers erscheint.

Beim Speichern eines Objekts in die Quarantäne wird das Objekt verschoben, nicht kopiert: Das Objekt wird von dem entsprechenden Laufwerk oder aus einer E-Mail-Nachricht gelöscht und im Quarantäneordner gespeichert. Die unter Quarantäne stehenden Dateien werden in einem speziellen Format gespeichert und stellen keine Gefahr dar.

15.1.1. Aktionen mit Objekten in der Quarantäne

Die Gesamtzahl der Objekte, die in die Quarantäne verschoben wurden, wird im Abschnitt **Datenverwaltung** des Programmhauptfensters genannt. Auf der rechten Seite des Hauptfensters befindet sich der spezielle Block **Quarantäne**, der folgende Daten enthält:

- Anzahl der möglicherweise infizierten Objekte, die während der Arbeit von Kaspersky Anti-Virus gefunden wurden.

- aktuelle Größe des Speichers.

Mit dem Link Leeren können alle Quarantäneobjekte gelöscht werden. Beachten Sie, dass dabei auch die Objekte des Backups und die Berichtsdateien gelöscht werden.

Um zu den Quarantäneobjekten zu wechseln,

verwenden Sie den Link Quarantäne.

Auf der Registerkarte **Quarantäne** (s. Abb. 57) können Sie folgende Aktionen vornehmen:

- Verschieben einer Datei in die Quarantäne, wenn Sie vermuten, dass die Datei von einem Virus infiziert ist, den das Programm nicht finden konnte. Klicken Sie dazu auf die Schaltfläche **Hinzufügen** und geben Sie im standardmäßigen Auswahlfenster die betreffende Datei an. Sie wird mit dem Status *Vom Benutzer hinzugefügt* zur Liste hinzugefügt.

> **Hinweis**
>
> Wenn eine Datei, die manuell in die Quarantäne verschoben wurde, bei einer folgenden Untersuchung als virenfrei erkannt wird, ändert sich ihr Status nicht gleich nach der Untersuchung in *ok*. Der Status ändert sich nur dann sofort, wenn die Untersuchung mindestens drei Tage, nachdem die Datei unter Quarantäne gestellt wurde, stattfindet.

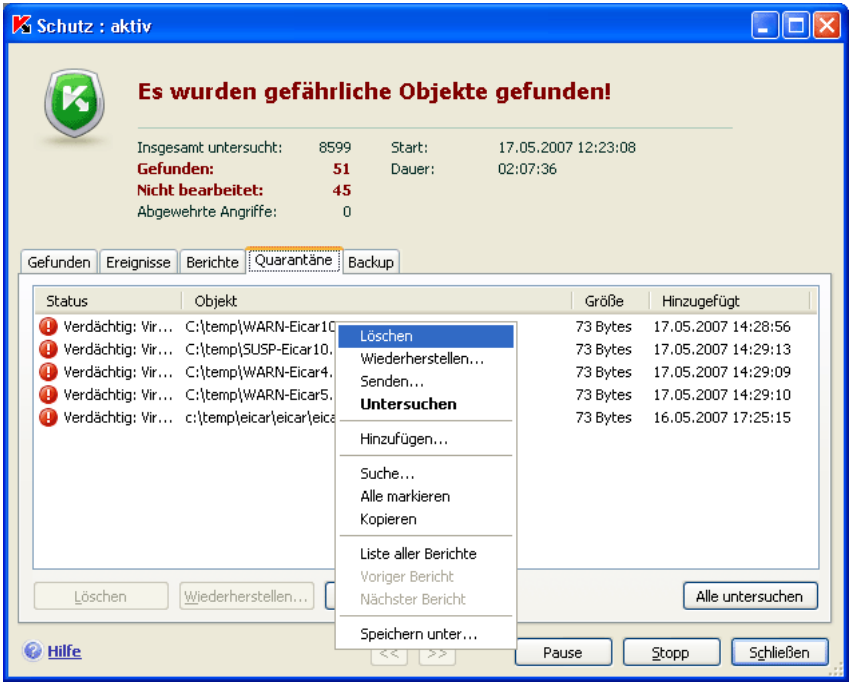


Abbildung 57. Liste der Quarantäneobjekte

- Alle möglicherweise infizierten Quarantäneobjekte unter Verwendung der aktuellen Version der Programm-Datenbanken untersuchen und desinfizieren. Klicken Sie dazu auf die Schaltfläche **Alle untersuchen**.

  Aufgrund der Untersuchung und Desinfektion eines beliebigen Quarantäne-Objekts kann sich sein Status in *infiziert*, *möglicherweise infiziert*, *Fehlalarm*, *ok* u.a. ändern.

  Der Objektstatus *infiziert* bedeutet, dass das Objekt als infiziert erkannt wurde, die Desinfektion aber fehlgeschlagen ist. Wir empfehlen, Objekte mit diesem Status zu löschen.

  Alle Objekte mit dem Status *Fehlalarm* können bedenkenlos wiederhergestellt werden, weil ihr vorheriger Status *möglicherweise infiziert* bei einer erneuten Untersuchung vom Programm nicht bestätigt wurde.

- Dateien wiederherstellen – entweder in einem vom Benutzer gewählten Ordner oder in den Ordnern, aus denen sie (standardmäßig) in die Quarantäne verschoben wurden. Zum Wiederherstellen eines Objekts markieren Sie es in der Liste und klicken Sie auf **Wiederherstellen**. Bei der

Wiederherstellung von Objekten, die aus Archiven, Mail-Datenbanken und Mail-Format-Dateien in die Quarantäne verschoben wurden, muss zusätzlich der Ordner angegeben werden, in dem sie wiederhergestellt werden sollen.

> **Hinweis**
>
> Es wird empfohlen, nur Objekte mit dem Status *Fehlalarm*, *ok* und *desinfiziert* wiederherzustellen, da die Wiederherstellung anderer Objekte zur Infektion Ihres Computers führen kann!

- Ein beliebiges Quarantäne-Objekt oder eine Gruppe ausgewählter Objekte löschen. Löschen Sie nur die Objekte, die nicht desinfiziert werden können. Klicken Sie auf die Schaltfläche **Löschen**, um Objekte zu löschen.

15.1.2. Konfiguration der Quarantäne-Einstellungen

Sie können folgende Parameter für das Erstellen und die Arbeit der Quarantäne anpassen:

- Auswahl des Modus zur automatischen Untersuchung von Objekten in der Quarantäne nach jedem Update der Programm-Datenbanken (Details s. Pkt. 13.3.3 auf S. 182).

  > **Achtung!**
  >
  > Das Programm kann die Quarantäneobjekte nicht unmittelbar nach der Aktualisierung der Datenbanken untersuchen, wenn Sie in diesem Moment mit der Quarantäne arbeiten.

- Festlegen der maximalen Speicherdauer für Objekte in der Quarantäne.

  Standardmäßig beträgt die Speicherdauer für Quarantäneobjekte 30 Tage. Danach werden die Objekte gelöscht. Sie können die maximale Speicherdauer für möglicherweise infizierte Objekte ändern oder diese Beschränkung ganz aufheben.

Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie den Abschnitt **Datenverwaltung**.

2. Legen Sie im Block **Quarantäne und Backup** (s. Abb. 58) den Zeitraum fest, nach dem Quarantäneobjekte automatisch gelöscht werden sollen.

Abbildung 58. Anpassen der Speicherdauer für Quarantäneobjekte

15.2. Sicherungskopien gefährlicher Objekte

Bei der Desinfektion von Objekten kann es vorkommen, dass es nicht gelingt, die Objekte vollständig zu erhalten. Wenn ein desinfiziertes Objekt wichtige Informationen enthielt, die aufgrund der Desinfektion vollständig oder teilweise verloren gingen, kann versucht werden, das ursprüngliche Objekt über seine Sicherungskopie wiederherzustellen.

Eine **Sicherungskopie** ist die Kopie eines gefährlichen Originalobjekts, die bei der ersten Desinfektion oder beim Löschen des Objekts erstellt und im Backup gespeichert wird.

Der **Backup-Speicher** ist ein spezieller Speicher, der die Sicherungskopien gefährlicher Objekte enthält, die bearbeitet oder gelöscht werden. Die Hauptfunktion des Backups besteht in der Möglichkeit, das ursprüngliche Objekt jederzeit wiederherzustellen. Die Sicherungskopien werden im Backup in einem speziellen Format gespeichert und stellen keine Gefahr dar.

15.2.1. Aktionen mit Sicherungskopien

Die Gesamtzahl der Sicherungskopien von Objekten, die sich im Backup befinden, wird im Abschnitt **Datenverwaltung**des Programmhauptfensters genannt. Auf der rechten Seite des Hauptfensters befindet sich der spezielle Block **Backup**, der folgende Daten enthält:

- Anzahl der Kopien von möglicherweise infizierten Objekten, die während der Arbeit von Kaspersky Anti-Virus angelegt wurden.
- aktuelle Größe des Backup-Speichers.

Mit dem Link Leeren können alle Sicherungskopien aus dem Backup gelöscht werden. Beachten Sie, dass dabei auch die Objekte aus der Quarantäne und die Berichtsdateien gelöscht werden.

Um zu den Kopien der gefährlichen Objekte zu wechseln,

verwenden Sie den Link Backup.

Im mittleren Bereich der Registerkarte **Backup** (s. Abb. 59) befindet sich eine Liste der Sicherungskopien. Für jede Kopie werden folgende Informationen angegeben: vollständiger Name des Objekts mit Pfadangabe des ursprünglichen Speicherorts, Status des Objekts, der ihm aufgrund der Untersuchung zugewiesen wurde, und Größe.

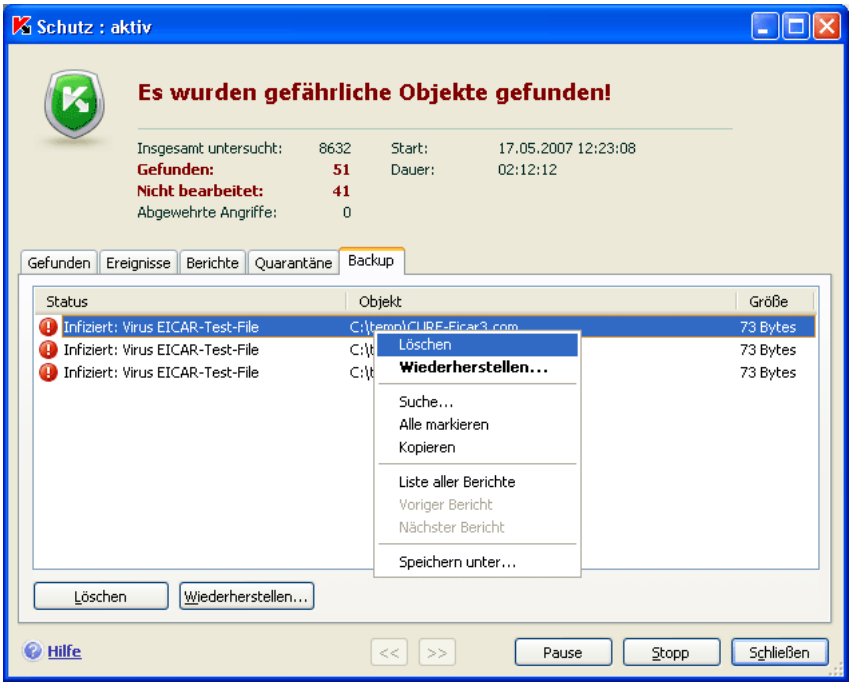


Abbildung 59. Sicherungskopien von gelöschten oder desinfizierten Objekten

Sie können ausgewählte Kopien mit Hilfe der Schaltfläche **Wiederherstellen** wiederherstellen. Das Objekt wird unter dem gleichen Namen aus dem Backup wiederhergestellt, den es vor der Desinfektion trug.

Wenn sich am ursprünglichen Speicherort ein Objekt mit dem gleichen Namen befindet (Diese Situation ist möglich, wenn ein Objekt wiederhergestellt wird, dessen Kopie vor der Desinfektion angelegt wurde), erscheint eine entsprechende Warnung auf dem Bildschirm. Sie können den Speicherort des wiederherzustellenden Objekts ändern oder es umbenennen.

Es wird empfohlen, das Objekt sofort nach der Wiederherstellung auf Viren zu untersuchen. Möglicherweise gelingt es, das Objekt mit den aktualisierten Programm-Datenbanken ohne Datenverlust zu desinfizieren.

Achtung!

Es wird davor gewarnt, Sicherungskopien von Objekten wiederherzustellen, wenn es nicht absolut erforderlich ist. Dies kann zur Infektion des Computers führen.

Es wird empfohlen, den Speicher in bestimmten Zeitabständen zu überprüfen und überflüssige Objekte mit Hilfe der Schaltfläche **Löschen** zu entfernen. Sie können das Programm auch so konfigurieren, dass die ältesten Kopien automatisch aus dem Speicher gelöscht werden (s. Pkt. 15.2.2 auf S. 195).

15.2.2. Konfiguration der Backup-Einstellungen

Sie können die maximale Speicherdauer der Kopien im Backup festlegen.

Standardmäßig beträgt die Speicherdauer für Kopien gefährlicher Objekte 30 Tage. Danach werden die Kopien gelöscht. Sie können die maximale Speicherdauer für Kopien ändern oder diese Beschränkung ganz aufheben. Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie den Abschnitt **Datenverwaltung**.
2. Legen Sie die Speicherdauer für Sicherungskopien im Block **Quarantäne und Backup** auf der rechten Seite des Fensters fest (s. Abb. 58).

15.3. Berichte

Die Arbeit jeder Komponente von Kaspersky Anti-Virus und die Ausführung jeder Aufgabe zur Virensuche und des Updates werden in einem Bericht aufgezeichnet.

Über die Gesamtzahl der Berichte, die bisher vom Programm erstellt wurden, sowie ihre Gesamtgröße in Bytes wird im Abschnitt **Datenverwaltung** des Programmhauptfensters informiert. Diese Informationen befinden sich im Block **Berichte**.

Um zur Anzeige der Berichte zu wechseln,

verwenden Sie den Link Berichte.

Dadurch wird das Fenster auf der Registerkarte **Berichte** geöffnet (s. Abb. 60). Hier befinden sich die neuesten Berichte für alle Komponenten und für die Aufgaben zur Virensuche und zum Update, die in der laufenden Sitzung von Kaspersky Anti-Virus gestartet wurden. Neben jeder Komponente und Aufgabe wird das Arbeitsergebnis genannt (beispielsweise *aktiv*, *Pause* oder *deaktiviert*). Wenn Sie den vollständigen Verlauf der Berichtserstellung für die laufende Programmsitzung lesen möchten, aktivieren Sie das Kontrollkästchen **Verlauf der Berichte anzeigen**.

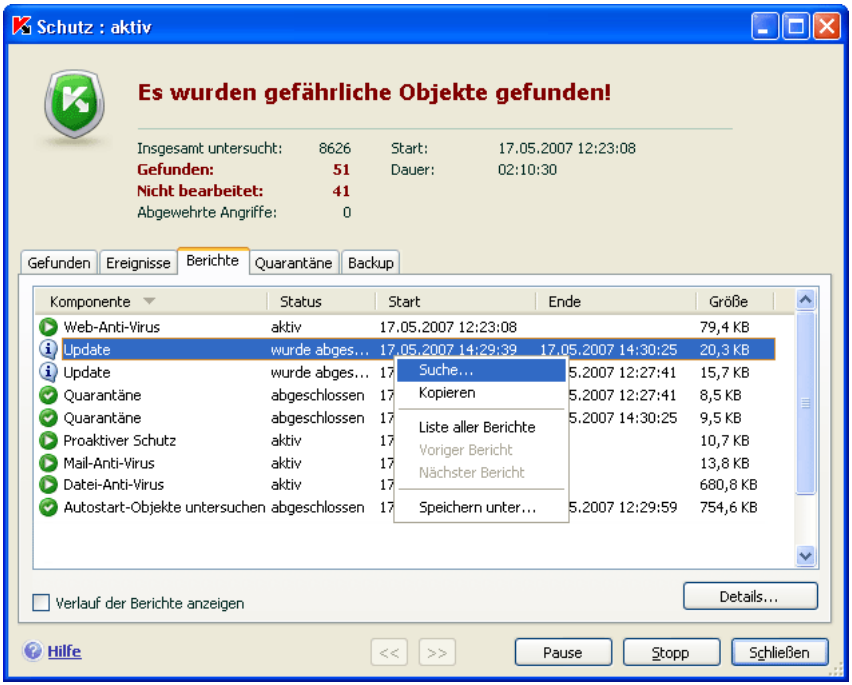


Abbildung 60. Berichte über die Arbeit der Programmkomponenten

Um alle Ereignisse anzuzeigen, die im Bericht über die Arbeit einer Komponente oder die Ausführung einer Aufgabe aufgezeichnet wurden,

wählen Sie den Namen der Komponente oder Aufgabe auf der Registerkarte **Berichte** und klicken Sie auf die Schaltfläche **Details**.

Dadurch wird ein Fenster geöffnet, das Detailinformationen über die Arbeit der gewählten Komponente oder Aufgabe enthält. Die Ergebnisstatistik der Arbeit befindet sich im oberen Bereich des Fensters, ausführliche Informationen befinden sich auf verschiedenen Registerkarten im mittleren Bereich. Abhängig von

der Komponente oder Aufgabe unterscheidet sich der Aufbau der Registerkarten:

- Die Registerkarte **Gefunden** enthält eine Liste der gefährlichen Objekte, die bei der Arbeit der Komponente oder beim Ausführen einer Untersuchungsaufgabe gefunden wurden.
- Die Registerkarte **Ereignisse** informiert über die Ereignisse bei der Arbeit einer Komponente oder Aufgabe.
- Die Registerkarte **Statistik** umfasst eine ausführliche Statistik aller untersuchten Objekte.
- Die Registerkarte **Einstellungen** enthält die Parameter, mit denen die Schutzkomponente, Aufgabe zur Virensuche oder das Update der Programm-Datenbanken arbeitet.
- Die Registerkarte **Registrierung** ist nur im Bericht des Proaktiven Schutzes vorhanden und enthält Informationen über alle Versuche zum Ändern der Systemregistrierung des Betriebssystems.

Sie können den gesamten Bericht in eine Textdatei importieren. Das kann beispielsweise von Nutzen sein, wenn bei der Arbeit einer Komponente oder bei der Aufgabenausführung ein Fehler aufgetreten ist, den Sie nicht selbständig beseitigen können, und deshalb die Hilfe des technischen Support-Services erforderlich ist. In diesem Fall wird der Bericht im Textformat an den Support-Service geschickt, damit unsere Spezialisten das Problem genau untersuchen und so schnell wie möglich lösen können.

Um einen Bericht in eine Textdatei zu importieren,

klicken Sie auf die Schaltfläche **Aktionen → Speichern unter** und geben Sie an, wo die Berichtsdatei gespeichert werden soll.

Klicken Sie zum Abschluss der Arbeit mit dem Bericht auf die Schaltfläche **Schließen**.

Alle Registerkarten des Berichts außer **Einstellungen** und **Statistik** verfügen über die Schaltfläche **Aktionen → Speichern unter**, mit deren Hilfe Sie eine Reihe von Aktionen mit den Objekten der Liste vornehmen können. Durch Klick auf diese Schaltfläche öffnet sich ein Kontextmenü mit folgenden Punkten (Die Auswahl der Menüpunkte unterscheidet sich in Abhängigkeit von der Komponente, deren Bericht Sie geöffnet haben. Unten werden alle möglichen Punkte genannt):

- **Desinfizieren** – Es wird versucht, das gefährliche Objekt zu desinfizieren. Wenn die Desinfektion des Objekts fehlschlägt, können Sie es entweder in der Liste belassen, um es später mit aktualisierten Programm-Datenbanken zu untersuchen, oder es löschen. Diese Aktion kann sowohl auf ein einzelnes Objekt der Liste als auch auf mehrere ausgewählte Objekte angewandt werden.

- **Löschen** - Das gefährliche Objekt aus dem Computer löschen.
- **Aus der Liste löschen**. Der Eintrag über den Fund des Objekts wird aus dem Bericht gelöscht.
- **Zur vertrauenswürdigen Zone hinzufügen** – Das Objekt wird den Schutzausnahmen hinzugefügt. Dabei wird ein Fenster mit der Ausnahmeregel für dieses Objekt geöffnet.
- **Alle desinfizieren** – Alle Objekte der Liste desinfizieren. Kaspersky Anti-Virus versucht, die Objekte unter Verwendung der Programm-Datenbanken zu bearbeiten.
- **Leeren** – Den Bericht über gefundene Objekte leeren. Dabei verbleiben alle gefundenen gefährlichen Objekte auf Ihrem Computer.
- **Datei anzeigen** – Öffnen von Microsoft Windows Explorer in dem Ordner, in dem sich das Objekt befindet.
- **Auf** http://www.viruslist.com/de **anschauen** – Zur Beschreibung des Objekts in der Viren-Enzyklopädie auf der Seite von Kaspersky Lab gehen.
- **Suche** – Die Bedingungen für die Suche nach einem Objekt (nach Name oder Status) in der Liste angeben.
- **Speichern unter** – Den Bericht im Textformat speichern.

Die Bearbeitung gefährlicher Objekte, die während der Arbeit von Kaspersky Anti-Virus gefunden wurden, erfolgt mit Hilfe der Schaltfläche **Desinfizieren** (für ein Objekt oder eine Gruppe ausgewählter Objekte) oder **Alle desinfizieren** (zur Bearbeitung aller Objekte in der Liste). Bei der Bearbeitung jedes Objekts erscheint auf dem Bildschirm eine Meldung, in der Sie aufgefordert werden, über die Aktion mit dem Objekt zu entscheiden.

Wenn Sie im Meldungsfenster das Kontrollkästchen **In allen ähnlichen Fällen anwenden** ankreuzen, wird die ausgewählte Aktion auf alle Objekte mit dem gleichen Status angewandt, die in der Liste vor dem Beginn der Bearbeitung ausgewählt wurden.

15.3.1. Konfiguration der Berichtsparameter

Zur Konfiguration der Parameter für das Erstellen und Speichern von Berichten

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie den Abschnitt **Datenverwaltung**.

2. Nehmen Sie im Block **Berichte** (s. Abb. 61) die erforderlichen Einstellungen vor:

   - Erlauben oder Verbieten Sie das Aufzeichnen von Ereignissen mit rein informativem Charakter in dem Bericht. In der Regel sind solche Ereignisse nicht für den Schutz wichtig. Aktivieren Sie das Kontrollkästchen **Informative Ereignisse protokollieren**, um das Speichern solcher Ereignisse zu erlauben.

   - Sie können festlegen, dass nur Ereignisse protokolliert werden, die beim letzten Start der Aufgabe eingetreten sind. Dadurch kann Festplattenplatz gespart werden, weil der Bericht eine geringere Größe besitzt. Wenn das Kontrollkästchen **Nur aktuelle Ereignisse speichern** aktiviert ist, werden die Informationen im Bericht bei jedem Neustart der Aufgabe aktualisiert. Allerdings werden nur Informationen mit rein informativem Charakter überschrieben.

   - Bestimmen Sie, wie lange Berichte gespeichert werden sollen. Der Standardwert für die Speicherdauer von Berichten beträgt 30 Tage. Sie können die Speicherdauer ändern oder diese Beschränkung völlig aufheben.

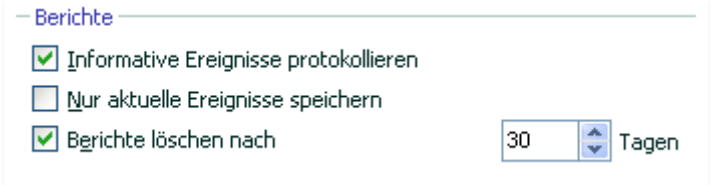


Abbildung 61. Einstellungen für das Erstellen von Berichten

15.3.2. Registerkarte *Gefunden*

Diese Registerkarte (s. Abb. 62) enthält eine Liste der gefährlichen Objekte, die von Kaspersky Anti-Virus gefunden wurden. Für jedes Objekt werden der vollständige Name und der Status angegeben, der ihm vom Programm bei der Untersuchung/Bearbeitung zugewiesen wurde.

Damit in der Liste nicht nur gefährliche Objekte, sondern auch Objekte, die erfolgreich desinfiziert wurden, angezeigt werden, aktivieren Sie das Kontrollkästchen **Desinfizierte Objekte anzeigen**.

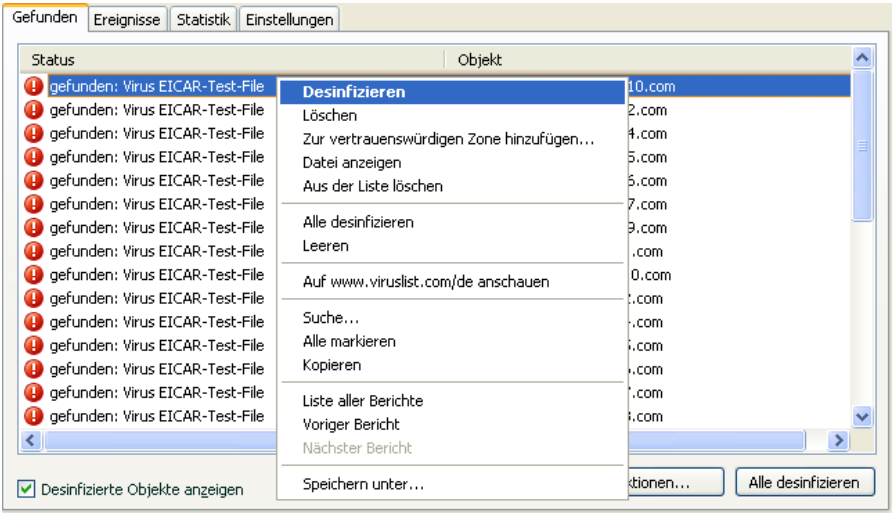


Abbildung 62. Liste der gefundenen gefährlichen Objekte

Die Bearbeitung gefährlicher Objekte, die während der Arbeit von Kaspersky Anti-Virus gefunden wurden, erfolgt mit Hilfe der Schaltfläche **Desinfizieren** (für ein Objekt oder eine Gruppe ausgewählter Objekte) oder **Alle desinfizieren** (zur Bearbeitung aller Objekte in der Liste). Bei der Bearbeitung jedes Objekts erscheint auf dem Bildschirm eine Meldung, in der Sie aufgefordert werden, über die Aktion mit dem Objekt zu entscheiden.

Wenn Sie im Meldungsfenster das Kontrollkästchen **In allen ähnlichen Fällen anwenden** ankreuzen, wird die ausgewählte Aktion auf alle Objekte mit dem gleichen Status angewandt, die vor dem Beginn der Bearbeitung in der Liste ausgewählt wurden.

15.3.3. Registerkarte *Ereignisse*

Auf dieser Registerkarte (s. Abb. 63) wird eine vollständige Liste aller wichtigen Ereignisse bei der Arbeit der Schutzkomponente oder beim Ausführen einer Aufgabe zur Virensuche oder zum Update geführt, wenn dem keine Regel zur Aktivitätskontrolle entgegensteht (s. Pkt. 10.1 auf S. 135).

Es gibt folgende Ereignistypen:

Kritische Ereignisse – Ereignisse mit kritischer Priorität, die auf Probleme bei der Arbeit des Programms oder auf Schwachstellen im Schutz Ihres Computers hinweisen. Beispiele: *Virus gefunden*, *Funktionsstörung*.

Wichtige Ereignisse – Ereignisse, die unbedingt beachtet werden müssen, weil Sie wichtige Situationen bei der Programmarbeit wiedergeben. Beispiel: *abgebrochen*.

Informative Ereignisse – Ereignisse mit informativem Charakter, die in der Regel keine wichtigen Informationen enthalten. Beispiele: *ok*, *nicht bearbeitet*. Diese Ereignisse erscheinen nur im Ereignisbericht, wenn das Kontrollkästchen ☑ **Alle Ereignisse anzeigen** aktiviert ist.

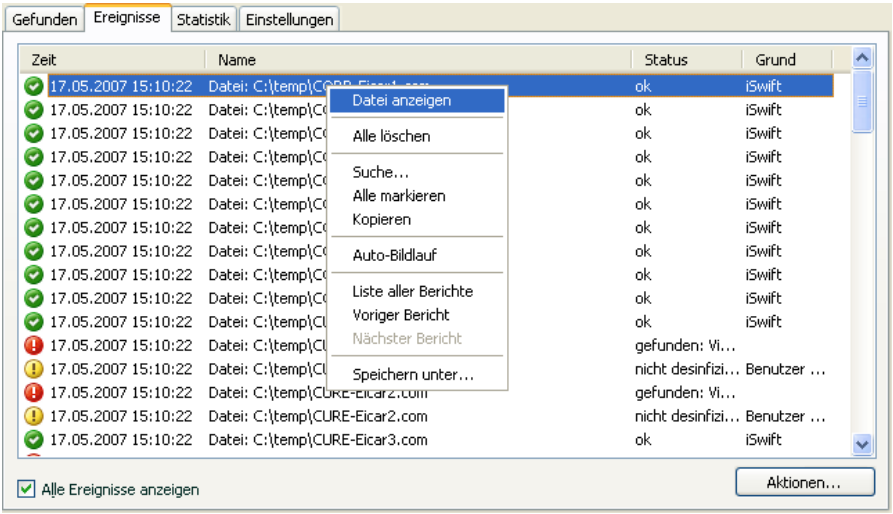


Abbildung 63. Ereignisse, die bei der Arbeit einer Komponente aufgetreten sind

Das Format der im Ereignisbericht enthaltenen Ereignisse kann in Abhängigkeit von der Komponente oder Aufgabe unterschiedlich sein. Für Update-Aufgaben wird beispielsweise angegeben:

- Ereignisname
- Name des Objekts, für das dieses Ereignis aufgezeichnet wurde.
- Zeitpunkt, zu dem das Ereignis eintrat.
- Größe der heruntergeladenen Datei.

Für eine Aufgabe zur Virensuche enthält der Ereignisbericht den Namen des untersuchten Objekts und den Status, der dem Objekt aufgrund der Untersuchung/Bearbeitung zugewiesen wurde.

15.3.4. Registerkarte *Statistik*

Eine ausführliche Statistik über die Arbeit der Komponente oder die Ausführung der Aufgabe zur Virensuche wird auf dieser Registerkarte aufgezeichnet (s. Abb. 64). Hier können Sie erfahren:

- Wie viele Objekte während der laufenden Sitzung der Komponente oder bei der Aufgabenausführung auf das Vorhandensein gefährlicher Objekte untersucht wurden. Außerdem wird die Anzahl der untersuchten Archive, gepackten Dateien, kennwortgeschützten und beschädigten Objekte angegeben.
- Wie viele gefährliche Objekte gefunden wurden. Wie viele davon nicht desinfiziert, gelöscht und in die Quarantäne verschoben wurden.

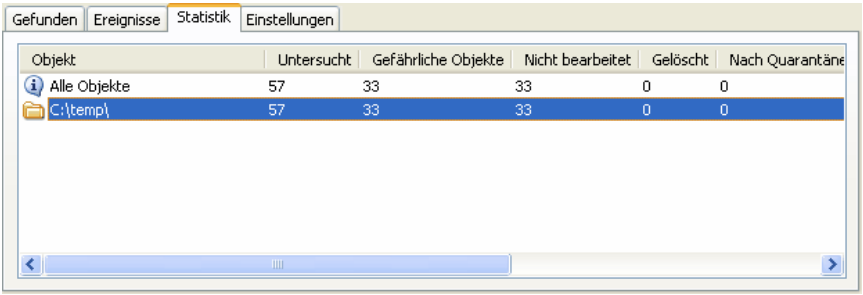


Abbildung 64. Statistik über die Arbeit einer Komponente

15.3.5. Registerkarte *Einstellungen*

Die Registerkarte **Einstellungen** (s. Abb. 65) enthält eine vollständige Übersicht der Parameter, mit denen die Schutzkomponente arbeitet oder die Untersuchungsaufgabe bzw. das Programm-Update ausgeführt wird. Sie können erfahren, welche Schutzstufe die Arbeit der Komponente bietet oder auf welcher Stufe die Virensuche ausgeführt wird, welche Aktion mit einem gefährlichen Objekt ausgeführt wird oder welche Einstellungen beim Programm-Update verwendet werden, usw. Um zur Konfiguration der Parameter zu wechseln, verwenden Sie den Link Einstellungen ändern.

Für die Aufgaben zur Virensuche können zusätzliche Ausführungsbedingungen festgelegt werden:

- Ausführungspriorität der Untersuchungsaufgabe bei Auslastung des Prozessors festlegen. Standardmäßig ist das Kontrollkästchen ☑ **Ressourcen für andere Anwendungen freigeben** aktiviert. Das Programm überwacht dabei das Auslastungsniveau des Prozessors und der

Laufwerkssubsysteme im Hinblick auf die Aktivität anderer Anwendungen. Wenn das Auslastungsniveau wesentlich ansteigt und die normale Arbeit der Benutzeranwendungen stört, beendet das Programm die Aktivität zur Ausführung der Untersuchungsaufgaben. Dies führt zur Verlängerung der Untersuchungszeit und zur Überlassung von Ressourcen an Benutzeranwendungen.

- Modus für die Arbeit des Computers nach dem Abschluss der Untersuchungsaufgabe bestimmen. Sie können festlegen, das der Computer nach Untersuchungsende ausgeschaltet oder neu gestartet wird oder in den Standbymodus oder Ruhemodus wechselt. Klicken Sie mit der linken Maustaste auf den Hyperlink, bis er den gewünschten Wert annimmt.

  Diese Option ist beispielsweise dann von Nutzen, wenn Sie die Virenuntersuchung des Computers kurz vor Feierabend starten und nicht auf deren Abschluss warten möchten.

  Die Verwendung dieser Option erfordert allerdings folgende zusätzlichen Vorbereitungen: Vor dem Untersuchungsstart muss die Kennwortabfrage bei der Objektuntersuchung deaktiviert werden, falls diese aktiviert war, und der Modus zur automatischen Bearbeitung gefährlicher Objekte muss festgelegt werden. Dadurch wird der interaktive Funktionsmodus des Programms abgeschaltet. Das Programm führt keine Anfragen durch, welche Ihre Reaktion erfordern und den Untersuchungsvorgang unterbrechen.

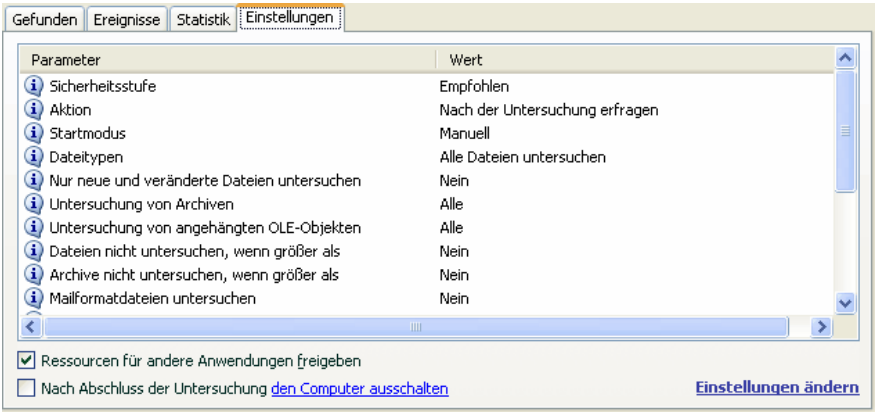


Abbildung 65. Einstellungen für die Arbeit einer Komponente

15.3.6. Registerkarte *Registrierung*

Die Operationen mit Registrierungsschlüsseln, deren Ausführung seit dem Programmstart versucht wurde, werden auf der Registerkarte **Registrierung** (s. Abb. 66) festgehalten, wenn die Protokollierung nicht durch eine Regel untersagt wird (s. Pkt. 10.3.2 auf S. 147).

Auf der Registerkarte werden der vollständige Name, Wert und Datentyp des Schlüssels sowie Angaben über die auszuführende Operation (versuchte Aktion, Zeitpunkt und ob die Aktion erlaubt wurde) angegeben.

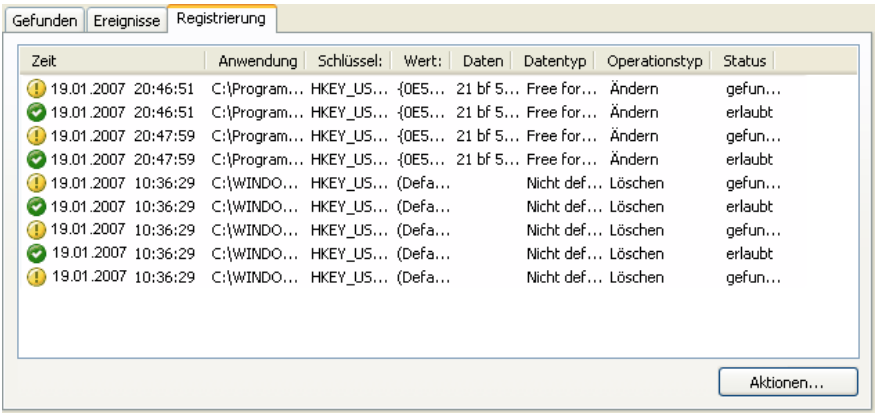

Gefunden
Ereignisse
Registrierung
Zeit
Anwendung
Schlüssel:
Wert:
Daten
Datentyp
Operationstyp
Status
19.01.2007 20:46:51 C:\Program... HKEY_US... {0E5... 21 bf 5... Free for... Ändern gefun...
19.01.2007 20:46:51 C:\Program... HKEY_US... {0E5... 21 bf 5... Free for... Ändern erlaubt
19.01.2007 20:47:59 C:\Program... HKEY_US... {0E5... 21 bf 5... Free for... Ändern gefun...
19.01.2007 20:47:59 C:\Program... HKEY_US... {0E5... 21 bf 5... Free for... Ändern erlaubt
19.01.2007 10:36:29 C:\WINDO... HKEY_US... (Defa... Nicht def... Löschen gefun...
19.01.2007 10:36:29 C:\WINDO... HKEY_US... (Defa... Nicht def... Löschen erlaubt
19.01.2007 10:36:29 C:\WINDO... HKEY_US... (Defa... Nicht def... Löschen gefun...
19.01.2007 10:36:29 C:\WINDO... HKEY_US... (Defa... Nicht def... Löschen erlaubt
19.01.2007 10:36:29 C:\WINDO... HKEY_US... (Defa... Nicht def... Löschen gefun...
Aktionen...

Abbildung 66. Ereignisse, die das Lesen und die Veränderung der Systemregistrierung betreffen

15.4. Notfall-CD zur Systemwiederherstellung

Das Programm Kaspersky Anti-Virus enthält einen Dienst zum Erstellen einer Notfall-CD zur Systemwiederherstellung.

Die Notfall-CD soll zur Wiederherstellung der Funktionsfähigkeit des Systems nach einem Virusangriff dienen, durch den Systemdateien des Betriebssystems beschädigt wurden und der Computer nicht mehr hochgefahren werden kann. Die Notfall-CD enthält:

- Systemdateien für Microsoft Windows XP Service Pack 2
- eine Auswahl von Dienstprogrammen zur Betriebssystemdiagnose
- Dateien des Programms Kaspersky Anti-Virus

- Dateien, welche die Programm-Datenbanken enthalten

Um eine Notfall-CD zu erstellen:

1. Öffnen Sie das Programmhauptfenster und wählen Sie den Abschnitt **Virensuche**.
2. Klicken Sie auf den Link Notfall-CD erstellen, um den Vorgang zum Erstellen der CD zu starten.

Achtung!

Die Notfall-CD dient ausschließlich für den Computer, auf welchem sie erstellt wurde. Die Verwendung der CD auf anderen Computern kann unvorhersehbare Folgen haben, weil sie Informationen über die Parameter des konkreten Computers enthält (z.B. Informationen über Bootsektoren).

Achtung!

Die Option zum Erstellen einer Notfall-CD ist nur verfügbar, wenn die Anwendung auf einem Computer mit dem Betriebssystem Microsoft Windows XP oder Microsoft Windows Vista installiert ist. Auf Computern mit anderen unterstützten Systemen, darunter auch Microsoft Windows XP Professional x64 Edition und Microsoft Windows Vista x64, ist das Erstellen der CD nicht vorgesehen.

15.4.1. Erstellen einer Notfall-CD

Achtung!

Zum Erstellen einer Notfall-CD zur Systemwiederherstellung müssen Sie über eine Installations-CD für Microsoft Windows XP Service Pack 2 verfügen.

Die Notfall-CD wird mit Hilfe des Spezialprogramms **PE Builder** erstellt.

Achtung!

Um mit Hilfe von PE Builder eine CD zu erstellen, muss dieses Programm vorher auf dem Computer installiert werden.

Beim Erstellen der Notfall-CD zur Systemwiederherstellung werden Sie von einem speziellen Assistenten begleitet, der aus einer Reihe von Fenstern (Schritten) besteht. Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Weiter** und **Zurück**, zum Abschluss der Arbeit des Assistenten die Schaltfläche

Fertig stellen. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf die Schaltfläche **Abbrechen** beendet werden.

Schritt 1. Vorbereitung zum Schreiben

Um die Notfall-CD für die Systemwiederherstellung zu erstellen, geben Sie die Pfade der folgenden Ordner an:

- Installationsorder des Programms von PE Builder.
- Ordner, in dem die Dateien für die Notfall-CD vor dem Schreiben der CD gespeichert werden sollen.

  Wenn Sie die CD nicht zum ersten Mal erstellen, enthält dieser Ordner bereits eine Auswahl von Dateien, die beim vorigen Mal gespeichert wurden. Aktivieren Sie das entsprechende Kontrollkästchen, um die früher gespeicherten Dateien zu verwenden.

  > **Hinweis**
  >
  > Beachten Sie, dass die früher gespeicherte Version der Notfall-CD-Dateien eine veraltete Version der Programm-Datenbanken enthält. Um die Virenanalyse des Computers und die Systemwiederherstellung auf optimale Weise zu gewährleisten, wird empfohlen, die Bedrohungssignaturen zu aktualisieren und eine neue Version der Notfall-CD zu erstellen.

- Installations-CD für Microsoft Windows XP Service Pack 2.

  Klicken Sie auf die Schaltfläche **Weiter**, nachdem Sie die erforderlichen Pfadangaben gemacht haben. Dadurch wird das Programm PE Builder gestartet und der Vorgang zum Erstellen der Dateien für die Notfall-CD beginnt. Warten Sie, bis der Vorgang abgeschlossen wird. Dies kann einige Minuten in Anspruch nehmen.

Schritt 2. Erstellen einer ISO-Datei

Nachdem das Programm PE Builder die Dateien für die Notfall-CD zur Systemwiederherstellung vorbereitet hat, wird das Fenster **Erstellen der ISO-Datei** geöffnet.

Die ISO-Datei ist ein Image der zu erstellenden CD in Form eines Archivs. Dateien im ISO-Format werden von den meisten CD-Brennprogrammen (beispielsweise Nero) unterstützt.

Wenn Sie nicht zum ersten Mal eine Notfall-CD erstellen, können Sie die Verwendung der vorherigen Version der ISO-Datei wählen. Wählen Sie dazu die Variante **Vorhandene ISO-Datei verwenden**.

Schritt 3. Schreiben der CD

In diesem Fenster fordert der Assistent Sie auf anzugeben, wann die Dateien der Notfall-CD zur Systemwiederherstellung auf die CD geschrieben werden sollen: jetzt oder später.

Wenn Sie das unverzügliche Schreiben der CD wählen, geben Sie an, ob der Inhalt der CD vor dem Schreiben gelöscht werden soll. Aktivieren Sie dazu das entsprechende Kontrollkästchen. Diese Option steht nur zur Verfügung, wenn die CD wiederholt mit Daten beschrieben werden kann (CD-RW).

Durch Klick auf die Schaltfläche **Weiter** wird der Vorgang zum Schreiben der CD gestartet. Warten Sie bis zum Abschluss des Vorgangs. Dies kann einige Minuten in Anspruch nehmen.

Schritt 4. Abschluss des Erstellens der Notfall-CD zur Systemwiederherstellung

In diesem Fenster informiert der Assistent Sie darüber, dass die Notfall-CD erfolgreich erstellt wurde.

15.4.2. Verwendung der Notfall-CD

Achtung!

Beachten Sie, dass Kaspersky Anti-Virus im Notfall-Modus zur Systemwiederherstellung nur arbeitet, wenn das Hauptfenster geöffnet ist. Beim Schließen des Programmhauptfensters wird das Programm beendet.

Hinweis

In dem Programm Bart PE, das standardmäßig installiert wird, werden keine chm-Dateien und Webbrowser unterstützt. Deshalb stehen im Notfall-Modus zur Systemwiederherstellung das Hilfesystem von Kaspersky Anti-Virus und die Links auf der Programmoberfläche nicht zur Verfügung.

Sollte eine Situation eintreten, in der das Betriebssystem aufgrund eines Virusangriffs nicht mehr gestartet werden kann, dann gehen Sie folgendermaßen vor:

1. Erstellen Sie unter Verwendung des Programms Kaspersky Anti-Virus auf einem virenfreien Computer eine Notfall-CD.
2. Legen Sie die Notfall-CD zur Systemwiederherstellung in das CD-Laufwerk des infizierten Computers ein und starten Sie ihn neu.

Dadurch wird das Betriebssystem Microsoft Windows XP SP2 mit dem Interface des Programms Bart PE gestartet.
Das Programm Bart PE besitzt eine integrierte Netzwerkunterstützung für die Verwendung eines lokalen Netzwerks. Beim Start des Programms erfolgt auf dem Bildschirm eine Bestätigungsabfrage. Bestätigen Sie das Aktivieren der Netzwerkunterstützung, wenn Sie vor der Untersuchung des Computers planen, die Programm-Datenbanken aus dem lokalen Netzwerk zu aktualisieren. Wenn kein Update erforderlich ist, lehnen Sie das Aktivieren der Netzwerkunterstützung ab.

3. Führen Sie den Befehl **GO→Programs→Kaspersky Anti-Virus 7.0→Start** aus, um Kaspersky Anti-Virus zu starten.

   Dadurch wird das Hauptfenster von Kaspersky Anti-Virus geöffnet. Im Notfall-Modus zur Systemwiederherstellung sind nur die Aufgaben zur Virensuche und (falls die Netzwerkunterstützung von Bart PE aktiviert ist) zum Update der Programm-Datenbanken aus einem lokalen Netzwerk verfügbar.

4. Starten Sie die Virenuntersuchung des Computers.

Achtung!

Beachten Sie, dass für die Untersuchung standardmäßig die Datenbanken verwendet werden, die am Erstellungsdatum der Notfall-CD aktuell waren. Aus diesem Grund wird empfohlen, die Datenbanken der Bedrohungssignaturen vor Untersuchungsbeginn zu aktualisieren.

Außerdem ist zu beachten, dass die aktualisierten Programm-Datenbanken von der Anwendung nur in der laufenden Sitzung mit der Notfall-CD verwendet werden, d.h. bis zum Neustart des Computers.

Achtung!

Wenn bei der Untersuchung des Computers infizierte oder möglicherweise infizierte Objekte gefunden wurden, und diese aufgrund der Bearbeitung in die Quarantäne oder ins Backup verschoben wurden, wird empfohlen, die Bearbeitung dieser Objekte während der laufenden Sitzung mit der Notfall-CD abzuschließen.

Andernfalls gehen diese Objekte nach dem Neustart des Computers verloren.

15.5. Erstellen einer Liste der zu kontrollierenden Ports

Bei der Arbeit von Schutzkomponenten wie Mail-Anti-Virus und Web-Anti-Virus werden Datenströme kontrolliert, die mit bestimmten Protokollen übertragen und über bestimmte offene Ports Ihres Computers weitergeleitet werden. Mail-Anti-Virus analysiert beispielsweise die Informationen, die mit dem Protokoll SMTP übertragen werden, Web-Anti-Virus analysiert HTTP-Pakete.

Eine Liste der Ports, die gewöhnlich zur Übertragung von E-Mail und HTTP-Datenströmen benutzt werden, gehört zum Lieferumfang des Programms. Sie können einen neuen Port hinzufügen oder die Kontrolle eines bestimmten Ports deaktivieren und dadurch veranlassen, dass der Datenstrom, der über diesen Port geleitet wird, nicht auf gefährliche Objekte hin untersucht wird.

Gehen Sie folgendermaßen vor, um die Liste der zu kontrollierenden Ports zu bearbeiten:

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie den Abschnitt **Kontrolle des Datenverkehrs**.
2. Klicken Sie auf die Schaltfläche **Port-Einstellungen**.
3. Korrigieren Sie die Liste der zu kontrollierenden Ports im Fenster **Port-Einstellungen** (s. Abb. 67).

Dieses Fenster enthält eine Liste der Ports, die von Kaspersky Anti-Virus kontrolliert werden. Wählen Sie die Variante **Alle Ports überwachen**, damit alle offenen Ports des Netzwerks überwacht werden, oder wählen Sie **Nur ausgewählte Ports überwachen**, um die Liste der zu kontrollierenden Ports selbst anzupassen.

Um einen neuen Port zur Liste der zu kontrollierenden Ports hinzuzufügen,

1. Klicken Sie im Fenster zur Port-Konfiguration auf die Schaltfläche **Hinzufügen**.
2. Geben Sie in den entsprechenden Feldern des Fensters **Neuer Port** die Portnummer und seine Beschreibung an.

Auf Ihrem Computer kann beispielsweise ein nicht standardmäßiger Port für den Datentransfer mit einem entfernten Computer über das HTTP-Protokoll konfiguriert sein. Die Kontrolle des HTTP-Datenverkehrs erfolgt durch die Komponente Web-Anti-Virus. Damit dieser Datenverkehr auf das Vorhandensein von schädlichem Code analysiert wird, muss dieser Port zur Liste der zu kontrollierenden Ports hinzugefügt werden.

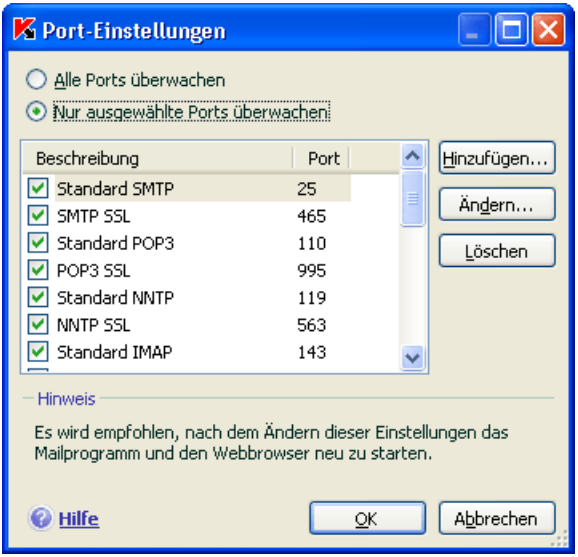


Abbildung 67. Liste der zu kontrollierenden Ports

Hinweis

Beim Start einer beliebigen Komponente öffnet das Programm Kaspersky Anti-Virus zur Überwachung aller eingehenden Verbindungen den Port 1110. Wenn dieser Port gerade von einer anderen Anwendung besetzt ist, wird Port 1111, 1112 usw. zur Überwachung gewählt.

Wenn das Programm Kaspersky Anti-Virus gleichzeitig mit der Firewall eines anderen Herstellers verwendet wird, müssen in den Einstellungen dieser Firewall Erlaubnisregeln für den Prozess *avp.exe* (interner Prozess von Kaspersky Anti-Virus) für alle aufgezählten Ports erstellt werden.

Beispielsweise kann in Ihrer Firewall eine Regel für den Prozess *iexplorer.exe* vorhanden sein, nach welcher diesem Prozess erlaubt wird, einen Verbindung auf Port 80 herzustellen.

Trotzdem fängt Kaspersky Anti-Virus die Anfrage für eine Verbindung ab, die vom Prozess *iexplorer.exe* auf Port 80 initiiert wird, und übergibt sie dem Prozess *avp.exe*, der versucht seinerseits eine Verbindung mit der aufgerufenen Webseite herzustellen. Wenn für den Prozess *avp.exe* keine Erlaubnisregel vorhanden ist, wird diese Anfrage von der Firewall blockiert und der Benutzer erhält keinen Zugriff auf die Webseite.

15.6. Untersuchung geschützter Verbindungen

Eine Verbindung unter Verwendung des SSL-Protokolls bietet den Schutz des Kommunikationskanals im Internet. Das SSL-Protokoll erlaubt es, die am Datenaustausch beteiligten Partner mit Hilfe elektronischer Zertifikate zu identifizieren, die zu übertragenden Daten zu verschlüsseln und die Datenintegrität beim Übertragungsvorgang zu gewährleisten.

Diese Besonderheiten des Protokolls werden von Angreifern zur Verbreitung von schädlichen Programmen benutzt, weil die meisten Antiviren-Produkte den SSL-Verkehr nicht untersuchen.

Kaspersky Anti-Virus bietet die Möglichkeit zur Virenuntersuchung des mit SSL-Protokoll übertragenen Datenstroms. Beim Versuch zur Verbindung mit einer Webressource im sicheren Modus erscheint auf dem Bildschirm eine Meldung (s. Abb. 68) mit einer Aktionsanfrage an den Benutzer.

Die Meldung enthält Informationen über das Programm, das die Verbindung im geschützten Modus initiiert hat, sowie die Remoteadresse und den Remoteport. Wählen Sie eine der folgenden Aktionen, um die Untersuchung fortzusetzen oder abzubrechen:

- **Bearbeiten** – Bei der Verbindung mit einer Webressource im geschützten Modus den Datenverkehr auf Viren untersuchen.
- **Überspringen** - Die Verbindung mit einer Webressource fortsetzen, ohne den Datenverkehr auf Viren zu untersuchen.

Damit die ausgewählte Aktion während der laufenden Sitzung des Webbrowsers auf alle Versuche zum Aufbau von SSL-Verbindungen angewandt wird, aktivieren Sie das Kontrollkästchen ☑ **Auf alle anwenden**.

Zur Untersuchung von verschlüsselten Verbindungen tauscht Kaspersky Anti-Virus das angeforderte Sicherheitszertifikat durch ein von ihm signiertes Zertifikat aus. In einigen Fällen akzeptieren Programme, die eine Verbindung herstellen, dieses Zertifikat nicht und die Verbindung kann deshalb nicht hergestellt werden. In solchen Fällen wird in der Meldung über die Untersuchung der geschützten Verbindung empfohlen, die Aktion **Überspringen** zu wählen:

- Bei einer Verbindung mit einer vertrauenswürdigen Webressource, beispielsweise mit der Webseite Ihrer Bank, auf der Sie Ihr eigenes Konto verwalten. In diesem Fall ist es wichtig, eine Bestätigung über die Echtheit des Bankzertifikats zu erhalten.
- Wenn das Programm, das eine Verbindung herstellt, eine Zertifikatsprüfung bei der angefragten Webressource vornimmt. Beispielsweise prüft

das Programm MSN Messenger beim Aufbau einer geschützten Verbindung mit einem Server die Echtheit der digitalen Microsoft Corporation-Signatur.

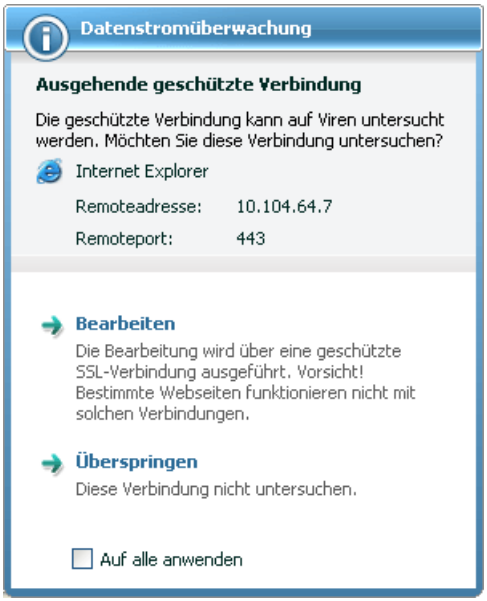

Datenstromüberwachung
Ausgehende geschützte Verbindung
Die geschützte Verbindung kann auf Viren untersucht werden. Möchten Sie diese Verbindung untersuchen?
Internet Explorer
Remoteadresse: 10.104.64.7
Remoteport: 443
Bearbeiten
Die Bearbeitung wird über eine geschützte SSL-Verbindung ausgeführt. Vorsicht! Bestimmte Webseiten funktionieren nicht mit solchen Verbindungen.
Überspringen
Diese Verbindung nicht untersuchen.
Auf alle anwenden

Abbildung 68. Meldung über den Fund einer SSL-Verbindung

Die Untersuchung von SSL-Verbindungen wird im Abschnitt **Kontrolle des Datenverkehrs** des Konfigurationsfensters der Anwendung angepasst (s. Abb. 69):

- **Alle geschützten Verbindungen untersuchen** – den gesamten Datenstrom, der mit dem SSL-Protokoll übertragen wird, auf Viren untersuchen.
- **Beim Fund eine neuen geschützten Verbindung fragen, ob die Untersuchung erforderlich ist** – Der Benutzer wird jedes Mal nach den gewünschten Aktionen gefragt, wenn versucht wird, eine SSL-Verbindung aufzubauen.
- **Geschützte Verbindungen nicht untersuchen** – den Datenstrom, der mit dem SSL-Protokoll übertragen wird, nicht auf Viren untersuchen.

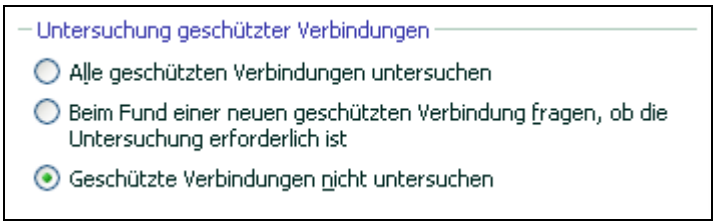

Untersuchung geschützter Verbindungen
Alle geschützten Verbindungen untersuchen
Beim Fund einer neuen geschützten Verbindung fragen, ob die Untersuchung erforderlich ist
Geschützte Verbindungen nicht untersuchen

Abbildung 69. Konfiguration der Untersuchung von geschützten Verbindungen

15.7. Konfiguration der Proxyserver-Parameter

Im Abschnitt **Proxyserver** des Konfigurationsfensters (s. Abb. 70) können Sie die Parameter der Verbindung mit dem Proxyserver anpassen (falls die Internetverbindung über einen Proxy erfolgt). Kaspersky Anti-Virus verwendet diese Daten bei der Arbeit einiger Echtzeitschutz-Komponenten und für das Update der Datenbanken und Programm-Module.

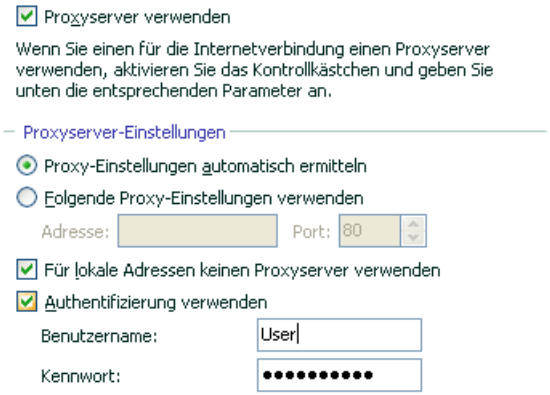

Proxyserver verwenden
Wenn Sie einen für die Internetverbindung einen Proxyserver verwenden, aktivieren Sie das Kontrollkästchen und geben Sie unten die entsprechenden Parameter an.
Proxyserver-Einstellungen
Proxy-Einstellungen automatisch ermitteln
Folgende Proxy-Einstellungen verwenden
Adresse:
Port: 80
Für lokale Adressen keinen Proxyserver verwenden
Authentifizierung verwenden
Benutzername: User
Kennwort: ••••••••••

Abbildung 70. Konfiguration der Proxyserver-Parameter

Wenn für die Internetverbindung ein Proxyserver verwendet wird, aktivieren Sie das Kontrollkästchen **Proxyserver verwenden** und passen Sie bei Bedarf folgende Parameter an:

- Wählen Sie, welche Proxyserver-Einstellungen verwendet werden sollen:

- **Proxy-Einstellungen automatisch ermitteln**. Bei Auswahl dieser Variante werden die Parameter des Proxyservers automatisch mit Hilfe des Protokolls WPAD (Web Proxy Auto-Discovery Protocol) ermittelt. Falls die Adresse mit diesem Protokoll nicht ermittelt werden kann, verwendet Kaspersky Anti-Virus die Proxy-Einstellungen, die in Microsoft Internet Explorer angegeben sind.
- **Folgende Proxy-Einstellungen verwenden** – Einen anderen Proxyserver verwenden, als jenen, der in den Verbindungseinstellungen des Browsers angegeben ist. Geben Sie im Feld **Adresse** die IP-Adresse oder den symbolischen Namen und im Feld **Port** den Port des Proxyservers an, der für das Programm-Update benutzt werden soll.

Damit beim Update aus einem lokalen Ordner oder Netzwerkordner kein Proxyserver verwendet wird, aktivieren Sie das Kontrollkästchen **Für lokale Adressen keinen Proxyserver verwenden**.

- Geben Sie an, ob auf dem Proxy eine Authentifizierung verwendet wird. Die *Authentifizierung* ist ein Vorgang, bei dem zum Zweck der Zugriffskontrolle die Anmeldungsdaten des Benutzers geprüft werden.

  Wenn für eine Verbindung mit dem Proxyserver die Authentifizierung erforderlich ist, aktivieren Sie das Kontrollkästchen **Authentifizierung verwenden** und geben Sie in den unten angebrachten Feldern den Benutzernamen und das Kennwort an. In diesem Fall wird zuerst die NTLM-Autorisierung, danach die BASIC-Autorisierung versucht.

  Wenn das Kontrollkästchen nicht aktiviert ist oder keine Daten angegeben werden, wird die NTLM-Autorisierung versucht, wobei das Benutzerkonto verwendet wird, in dessen Namen die Aufgabe (z.B. das Update, s. Pkt. 6.6 auf S. 70) gestartet wurde.

  Wenn die Autorisierung auf dem Proxyserver erforderlich ist, Sie aber den Benutzernamen und das Kennwort nicht angegeben haben oder der Proxyserver die angegebenen Daten aus einem beliebigen Grund nicht akzeptiert, erscheint beim Updatestart eine Anfrage nach Benutzername und Kennwort für die Autorisierung. Wenn die Autorisierung erfolgreich verläuft, werden der angegebene Benutzername und das Kennwort auch beim nächsten Update verwendet. Andernfalls werden die Autorisierungsparameter erneut abgefragt.

  Mit einem Klick auf die Schaltfläche Abbrechen im Fenster zur Abfrage der Parameter für die Autorisierung wird die aktuelle Updatequelle durch den nächsten Listeneintrag ersetzt und die Parameter für die Autorisierung, die in diesem Fenster oder in der Programmoberfläche stehen, werden ignoriert. Das heißt, es erfolgt ein Versuch der NTLM-Authentifizierung mit dem Benutzerkonto, in dessen Namen die Aufgabe gestartet wurde.

Wenn die Aktualisierung über einen ftp-Server erfolgt, findet die Verbindung mit dem Server standardmäßig im passiven Modus statt. Wenn bei dieser Verbindung ein Fehler auftritt, wird versucht, die Verbindung im passiven Modus auszuführen.

Der standardmäßig für den Verbindungsaufbau mit dem Updateserver vorgesehene Zeitraum beträgt eine Minute. Wenn nach Ablauf des Zeitraums keine Verbindung hergestellt wurde, wird versucht, eine Verbindung mit dem nächsten Server aufzubauen. Der Vorgang wird so fortgesetzt, bis der Verbindungsaufbau erfolgreich verläuft oder bis alle verfügbaren Updateserver aufgerufen wurden.

15.8. Konfiguration der Oberfläche von Kaspersky Anti-Virus

Kaspersky Anti-Virus bietet die Möglichkeit, das Aussehen des Programms zu verändern. Dazu können unterschiedliche grafische Elemente und Farbpaletten erstellt und verwendet werden. Zusätzlich besteht die Möglichkeit, aktive Elemente der Benutzeroberfläche anzupassen. Dazu zählen das Programmsymbol im Infobereich der Taskleiste von Microsoft Windows und Popup-Meldungen.

Gehen Sie folgendermaßen vor, um Oberfläche von Kaspersky Anti-Virus anzupassen:

Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie den Abschnitt **Ansicht** (s. Abb. 71).

Abbildung 71. Einstellungen für die Programmoberfläche

Auf der rechten Seite des Konfigurationsfensters können Sie festlegen:

- *Verwendung eigener grafischer Elemente und Farbpaletten auf der Programmoberfläche*.

  Standardmäßig werden für die grafische Programmoberfläche die Systemfarben und -stile verwendet. Sie können diese verwerfen. Deaktivieren Sie dazu das Kontrollkästchen **Systemfarben und –stile verwenden**. In diesem Fall werden die Schemen verwendet, die Sie bei der Konfiguration des Bildschirmdesigns angegeben haben.

  Alle auf der Oberfläche von Kaspersky Anti-Virus verwendeten Farben, Schriften, Piktogramme und Texte können verändert werden. Sie können eine individuelle grafische Oberfläche für das Programm erstellen und es in einer anderen Sprache lokalisieren. Um eine grafische Oberfläche zu verbinden, geben Sie das Verzeichnis mit ihren Parametern im Feld **Ordner mit Beschreibung der grafischen Oberfläche** an. Verwenden Sie zur Auswahl des Verzeichnisses die Schaltfläche **Durchsuchen**.

- *Transparenzstufe der Popupmeldungen.*

  Alle Operationen von Kaspersky Anti-Virus, die Ihre sofortige Aufmerksamkeit oder Entscheidung erfordern, besitzen das Aussehen einer Po-

pupmeldung über dem Programmsymbol im Infobereich der Taskleiste von Microsoft Windows. Die Meldungsfenster sind halbtransparent, damit sie Ihre Arbeit nicht stören. Wenn der Mauscursor auf das Meldungsfenster geführt wird, wird die Transparenz aufgehoben. Sie können die Transparenzstufe solcher Meldungen ändern. Verschieben Sie dazu den Zeiger auf der Skala **Transparenzkoeffizient** an die gewünschte Position. Deaktivieren Sie das Kontrollkästchen **Transparenz für Meldungsfenster verwenden**, wenn die Meldungen ohne Transparenz angezeigt werden sollen.

- *ob das Programmsymbol im Infobereich der Taskleiste von Microsoft Windows animiert werden soll oder nicht.*

  In Abhängigkeit von der ausgeführten Programmaktion ändert sich das Aussehen des Symbols. Wird beispielsweise die Untersuchung eines Skripts ausgeführt, dann erscheint im Hintergrund des Symbols ein kleines Piktogramm mit einem Skript. Bei der Untersuchung einer E-Mail-Nachricht erscheint das Piktogramm eines Briefs. Die Animation des Programmsymbols wird standardmäßig verwendet. Wenn Sie keine Animation wünschen, deaktivieren Sie das Kontrollkästchen **Animation des Symbols bei Aktivität (Datei-Untersuchung, Update usw.)**. In diesem Fall informiert das Symbol nur über den Schutzstatus Ihres Computers: Das farbige Symbol zeigt an, dass der Schutz aktiviert ist. Das Symbol ist grau, wenn der Schutz angehalten oder deaktiviert ist.

- *ob über das Eintreffen neuer Nachrichten von Kaspersky Lab informiert werden soll.*

  Standardmäßig erscheint beim Eintreffen von Nachrichten im Infobereich der Taskleiste von Microsoft Windows ein spezielles Symbol. Durch Klick auf das Symbol wird ein Fenster mit dem Nachrichtentext geöffnet. Wenn Sie die Anzeige des Symbols ausschalten möchten, deaktivieren Sie das Kontrollkästchen **Neuigkeiten durch das Taskleistensymbol melden**.

- *ob der Schutzindikator von Kaspersky Anti-Virus beim Hochfahren des Betriebssystems angezeigt werden soll oder nicht.*

  Standardmäßig erscheint dieser Indikator in der rechten oberen Bildschirmecke, wenn das Programm gestartet wird. Er informiert darüber, dass der Schutz Ihres Computers vor jeder Art von Bedrohung aktiviert ist. Wenn Sie den Schutzindikator nicht verwenden möchten, deaktivieren Sie das Kontrollkästchen **Symbol über dem Microsoft Windows-Begrüßungsbildschirm anzeigen**.

Achtung!

Beachten Sie, dass Änderungen der Interfaceparameter von Kaspersky Anti-Virus beim Wiederherstellen der Standardeinstellungen oder bei der Deinstallation der Anwendung nicht gespeichert werden.

15.9. Verwendung zusätzlicher Dienste

Kaspersky Anti-Virus bietet Ihnen an, folgende zusätzlichen Dienste zu verwenden (s. Abb. 72):

- Start von Kaspersky Anti-Virus beim Hochfahren des Betriebssystems (s. Pkt. 15.11 auf S. 231).
- Benachrichtigung des Benutzers über das Eintreten bestimmter Ereignisse bei der Arbeit des Programms (s. Pkt. 15.9.1 auf S. 219).
- Selbstschutz von Kaspersky Anti-Virus vor dem Beenden, Löschen und Verändern von Modulen, sowie Kennwortschutz für den Zugriff auf das Programm (s. Pkt. 15.9.2 auf S. 225).
- Export/Import von Funktionsparametern für Kaspersky Anti-Virus (s. Pkt. 15.9.3 auf S. 227).
- Wiederherstellen der Standardeinstellungen (s. Pkt. 15.9.4 auf S. 227).

Um zur Konfiguration der genannten Dienste zu gelangen,

öffnen Sie das Konfigurationsfenster des Programms und wählen Sie den Abschnitt Service.

Auf der rechten Seite können Sie festlegen, ob die Zusatzdienste bei der Programmarbeit verwendet werden sollen oder nicht.

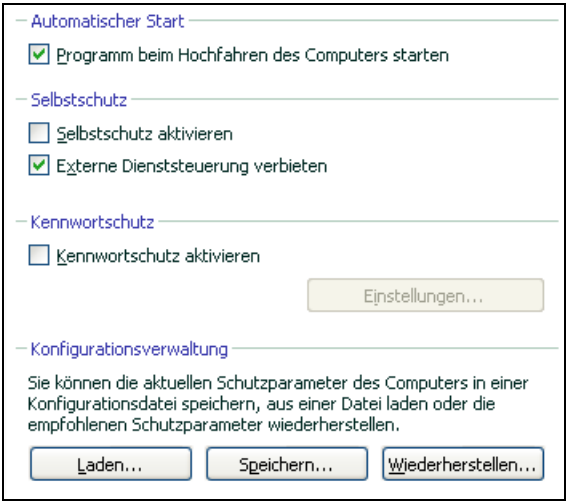


Abbildung 72. Konfiguration zusätzlicher Dienste

15.9.1. Benachrichtigungen über die Ereignisse von Kaspersky Anti-Virus

Bei der Arbeit von Kaspersky Anti-Virus treten unterschiedliche Ereignisse ein. Sie können informativen Charakter besitzen oder wichtige Informationen enthalten. Ein Ereignis kann beispielsweise über die erfolgreiche Aktualisierung des Programms informieren oder einen Fehler bei der Arbeit einer bestimmten Komponente festhalten, der dringend behoben werden muss.

Um sich über die Ereignisse bei der Arbeit von Kaspersky Anti-Virus informieren zu lassen, können Sie den Dienst für Benachrichtigungen verwenden.

Die Benachrichtigungen können durch eine der folgenden Methoden erfolgen:

- Popupmeldungen über dem Programmsymbol im Infobereich der Taskleiste von Microsoft Windows
- Tonsignale
- E-Mail-Nachrichten
- Protokollieren von Informationen im Ereignisbericht

Um diesen Dienst zu verwenden,

1. Aktivieren Sie im Block **Ereignisbenachrichtigung** des Konfigurationsfensters der Anwendung (s. Abb. 71) das Kontrollkästchen **Ereignisbenachrichtigung aktivieren**.
2. Legen Sie die Typen der Ereignisse von Kaspersky Anti-Virus fest, über deren Eintreten Sie benachrichtigt werden möchten, und wählen Sie eine Methode zum Senden der Benachrichtigungen (s. Pkt. 15.9.1.1 auf S. 220).
3. Passen Sie die Einstellungen für das Senden von Benachrichtigungen per E-Mail an, wenn Sie diese Benachrichtigungsmethode wünschen (s. Pkt. 15.9.1.2 auf S. 222).

15.9.1.1. Ereignistypen und Methoden zum Senden von Benachrichtigungen

Bei der Arbeit von Kaspersky Anti-Virus treten Ereignisse der folgenden Typen auf:

Kritische Ereignisse – Ereignisse mit kritischer Priorität. Es wird ausdrücklich empfohlen, sich über solche Ereignisse benachrichtigen zu lassen, weil sie auf Probleme bei der Arbeit des Programms oder auf Schwachstellen im Schutz Ihres Computers hinweisen. Beispiele: Die *Programm-Datenbanken sind beschädigt* oder *Die Gültigkeit des Schlüssels ist abgelaufen*.

Funktionsstörung – Ereignisse, die zur Funktionsunfähigkeit der Anwendung führen. Beispielsweise das Fehlen eines Schlüssels und der Programm-Datenbanken.

Wichtige Ereignisse – Ereignisse, die unbedingt beachtet werden müssen, weil Sie wichtige Situationen bei der Programmarbeit wiedergeben. Beispiele: *Alle Schutzkomponenten sind deaktiviert* oder *Der Computer wurde lange nicht untersucht*.

Informative Ereignisse – Ereignisse mit informativem Charakter, die in der Regel keine wichtigen Informationen enthalten. Beispiele: *Alle gefährlichen Objekte wurden neutralisiert*.

Um festzulegen, über welche Ereignisse und auf welche Weise Sie benachrichtigt werden möchten:

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie den Abschnitt **Ansicht** (s. Abb. 71).

2. Aktivieren Sie im Block **Ereignisbenachrichtigung** das Kontrollkästchen **Ereignisbenachrichtigung aktivieren** und gehen Sie mit Hilfe der Schaltfläche **Erweitert** zur ausführlichen Konfiguration über.

Im Fenster **Einstellungen für Benachrichtigungen über Ereignisse** (s. Abb. 73) können Sie folgende Benachrichtigungsmethoden für die oben genannten Ereignisse anpassen:

- *Popupmeldung* über dem Programmsymbol im Infobereich der Taskleiste von Microsoft Windows. Die Meldung enthält Informationen über das eingetretene Ereignis.

  Um diesen Typ der Benachrichtigung zu verwenden, aktivieren Sie das Kontrollkästchen in der Spalte **Anzeige** gegenüber dem Ereignis, über das Sie benachrichtigt werden möchten.

- *Tonsignale.*

  Wenn Sie möchten, dass die Benachrichtigung von einem Audiosignal begleitet wird, aktivieren Sie das Kontrollkästchen in der Spalte **Ton** neben dem Ereignis.

- *Benachrichtigung per E-Mail*.

  Um diesen Typ der Benachrichtigung zu verwenden, aktivieren Sie das Kontrollkästchen in der Spalte **E-Mail** gegenüber dem Ereignis, über das Sie benachrichtigt werden möchten, und passen Sie die Parameter für das Senden von Benachrichtigungen an (s. Pkt. 15.9.1.2 auf S. 222).

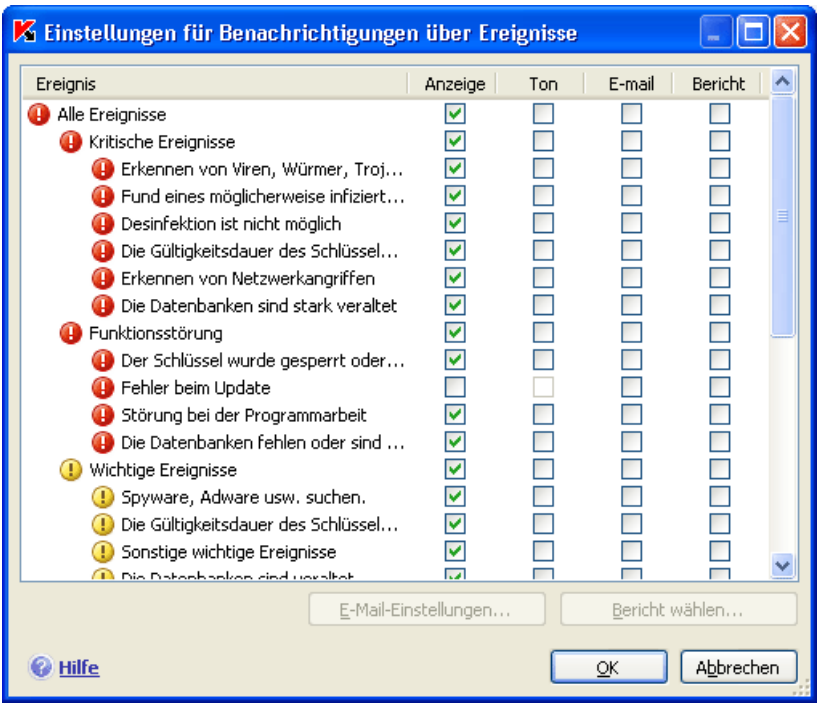


Abbildung 73. Ereignisse bei der Programmarbeit und entsprechende Benachrichtigungsmethoden

- *Protokollieren von Informationen im Ereignisbericht*.

  Damit Informationen über das Eintreten eines bestimmten Ereignisses im Bericht protokolliert werden, aktivieren Sie das Kontrollkästchen ☑ in der Spalte **Bericht** gegenüber dem Ereignis und passen Sie die Parameter für den Ereignisbericht an (s. Pkt. 15.9.1.3 auf S. 224).

15.9.1.2. Konfiguration des Sendens von Benachrichtigungen per E-Mail

Nachdem Sie die Ereignisse gewählt haben (s. Pkt. 15.9.1.1 auf S. 220), über deren Eintreten Sie per E-Mail benachrichtigt werden möchten, müssen Sie die folgenden Einstellungen für das Senden der Benachrichtigungen vornehmen:

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie den Abschnitt **Ansicht** (s. Abb. 71).

2. Klicken Sie im Block **Ereignisbenachrichtigung** auf die Schaltfläche **Erweitert**.

3. Aktivieren Sie im Fenster **Einstellungen für Benachrichtigungen über Ereignisse** (s. Abb. 73) in der Spalte **E-Mail** die Kontrollkästchen für die Ereignisse, bei deren Eintreten eine E-Mail-Benachrichtigung gesendet werden soll.

4. Legen Sie im Fenster (s. Abb. 74), das mit der Schaltfläche **Einstellungen für E-Mail-Benachrichtigungen** geöffnet wird, folgende Parameter für das Senden von E-Mail-Benachrichtigungen fest:

   - Geben Sie im Block **Benachrichtigungsabsender** die Parameter des Absenders der Benachrichtigungen an.

   - Geben Sie im Block **Benachrichtigungsempfänger** die E-Mail-Adresse an, an welche die Benachrichtigungen geschickt werden sollen.

   - Geben Sie im Block **Versandmodus** den Modus zum Senden der Benachrichtigungen per E-Mail an. Damit das Programm die Nachricht beim tatsächlichen Eintreten eines Ereignisses abschickt, wählen Sie **Bei Ereigniseintritt**. Erstellen Sie zur Benachrichtigung über Ereignisse nach einem bestimmten Zeitraum einen Zeitplan für das Senden von Nachrichten. Klicken Sie dazu auf die Schaltfläche **Ändern**. Standardmäßig erfolgt die Benachrichtigung täglich.

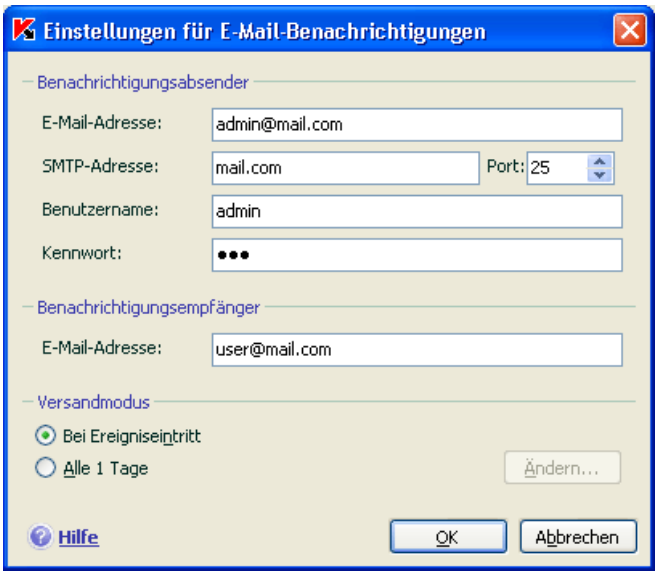


Abbildung 74. Einstellungen für E-Mail-Benachrichtigung

15.9.1.3. Parameter des Ereignisberichts

Um die Parameter des Ereignisberichts anzupassen:

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie den Abschnitt **Ansicht** (s. Abb. 71).
2. Klicken Sie im Block **Ereignisbenachrichtigung** auf die Schaltfläche **Erweitert**.

Wählen Sie im Fenster **Einstellungen für Benachrichtigungen über Ereignisse** für das gewünschte Ereignis die Option zur Protokollierung im Bericht und klicken Sie auf die Schaltfläche **Bericht wählen**.

Kaspersky Anti-Virus bietet die Möglichkeit, Informationen über Ereignisse, die bei der Arbeit der Anwendung eintreten, im allgemeinen Ereignisbericht von Microsoft Windows (**Anwendung**) oder in einem separaten Ereignisbericht von Kaspersky Anti-Virus (**Kaspersky Event Log**) aufzuzeichnen.

Zur Anzeige der Berichte dient das Microsoft Windows-Standardfenster **Ereignisanzeige**, das mit Hilfe des folgenden Befehls geöffnet wird: **Start → Einstellungen → Systemsteuerung → Verwaltung → Ereignisanzeige**.

15.9.2. Selbstschutz und Zugriffsbeschränkung für das Programm

Kaspersky Anti-Virus ist ein Programm, das den Computer vor schädlichen Programmen schützt, und wird dadurch selbst zu einem Ziel für schädliche Programme, die versuchen, die Arbeit des Programms zu blockieren oder es sogar vom Computer zu löschen.

Außerdem kann ein PC von verschiedenen Benutzern verwendet werden, deren Fertigkeiten im Umgang mit Computern möglicherweise nicht ausreichend sind. Der ungehinderte Zugriff auf das Programm und dessen Einstellungen kann das Sicherheitsniveau des Computers stark einschränken.

Um die Stabilität des Sicherheitssystems Ihres Computers zu gewährleisten, verfügt das Programm über Mechanismen zum Selbstschutz, zum Schutz vor externem Zugriff und zum Kennwortschutz für den Programmzugriff.

Achtung!

Für 64-Bit-Betriebssysteme und für Microsoft Windows Vista steht der Selbstschutzmechanismus der Anwendung nur im Hinblick auf Veränderungen oder das Löschen von Dateien auf der Festplatte sowie von Einträgen in der Systemregistrierung zur Verfügung.

Um die Selbstschutzmechanismen für das Programm zu aktivieren:

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie den Abschnitt **Service** (s. Abb. 72).
2. Nehmen Sie im Block **Selbstschutz** die entsprechenden Einstellungen vor:

   Selbstschutz aktivieren. Wenn dieses Kontrollkästchen aktiviert ist, wird der Mechanismus zum Schutz des Programms vor dem Verändern oder Löschen von eigenen Dateien auf der Festplatte, Prozessen im Arbeitsspeicher und Einträgen in der Systemregistrierung wirksam.

   Externe Dienststeuerung verbieten. Wenn dieses Kontrollkästchen aktiviert ist, wird jeder Versuch zur Fernsteuerung von Diensten der Anwendung blockiert.

   Um Programmen, die der Remote-Administration dienen (z.B. dem Programm RemoteAdmin), den Zugriff auf die Steuerung von Kaspersky Internet Security zu gewähren, müssen diese Programme zur Liste der vertrauenswürdigen Anwendungen hinzugefügt wer-

den und der Parameter **Anwendungsaktivität nicht kontrollieren** muss für sie aktiviert werden (s. Pkt. 6.9.2 auf S. 81).

Wird versucht, eine der oben genannten Aktionen auszuführen, dann erscheint eine Meldung über dem Programmsymbol im Infobereich der Taskleiste von Microsoft Windows (falls der Benachrichtigungsdienst nicht vom Benutzer deaktiviert wurde).

Um den Zugriff auf das Programm mit Hilfe eines Kennworts zu schützen, aktivieren Sie das Kontrollkästchen **Kennwortschutz aktivieren** im gleichnamigen Block und geben Sie im Fenster, das mit der Schaltfläche **Einstellungen** geöffnet wird, das Kennwort und den Bereich an, für den die Zugriffsbeschränkung gelten soll (s. Abb. 75). Sie können entweder alle Operationen mit dem Programm blockieren (unter Ausnahme der Arbeit mit Meldungen über den Fund gefährlicher Objekte) oder das Ausführen folgender Aktionen untersagen:

- Die Einstellungen für die Arbeit des Programms ändern.
- Die Arbeit von Kaspersky Anti-Virus beenden.
- Den Schutz Ihres Computers deaktivieren oder vorübergehend anhalten.

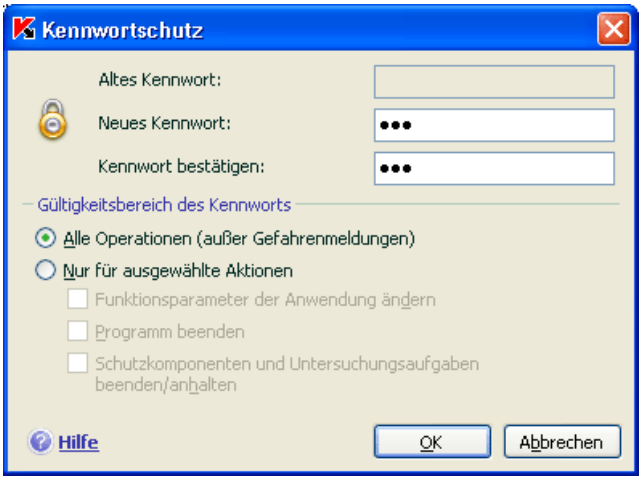


Abbildung 75. Einstellungen für den Kennwortschutz des Programms

Jede der oben genannten Aktionen führt zu einer Verringerung des Schutzniveaus Ihres Computers. Deshalb sollten Sie festlegen, welche Benutzer Ihres Computers berechtigt sein sollen, diese Aktionen auszuführen.

Beim Versuch eines beliebigen Benutzers Ihres Computers, die von Ihnen festgelegten Aktionen auszuführen, wird das Programm nun immer das Kennwort abfragen.

15.9.3. Export/Import der Einstellungen von Kaspersky Anti-Virus

Kaspersky Anti-Virus bietet Ihnen die Möglichkeit zum Exportieren und Importieren seiner Programmeinstellungen.

Diese Option kann beispielsweise von Nutzen sein, wenn Sie das Programm auf Ihrem PC zuhause und im Büro installiert haben. Sie können das Programm zu Hause entsprechend konfigurieren, die Einstellungen auf einer Diskette speichern und mit Hilfe der Importfunktion schnell auf Ihren Computer im Büro laden. Die Einstellungen werden in einer speziellen Konfigurationsdatei gespeichert.

Um die aktuellen Programmeinstellungen zu exportieren,

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie den Abschnitt **Service** (s. Abb. 72).
2. Klicken Sie im Block **Konfigurationsverwaltung** auf die Schaltfläche **Speichern**.
3. Geben Sie Name und Pfad der Konfigurationsdatei an.

Um die Programmeinstellungen aus einer Konfigurationsdatei zu importieren,

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie den Abschnitt **Service**.
2. Klicken Sie auf die Schaltfläche **Laden** und wählen Sie die Datei, aus der Sie die Parameter für Kaspersky Anti-Virus importieren möchten.

15.9.4. Wiederherstellen der Standardeinstellungen

Sie können jederzeit zu den empfohlenen Programmeinstellungen zurückkehren. Diese gelten als optimal und werden von den Kaspersky-Lab-Spezialisten empfohlen. Die Wiederherstellung der Einstellungen erfolgt mit Hilfe des Konfigurationsassistenten.

Um die Schutzeinstellungen wiederherzustellen,

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie den Abschnitt **Service** (s. Abb. 72).

2. Klicken Sie im Abschnitt **Konfigurationsverwaltung** auf die Schaltfläche **Wiederherstellen**.

Im folgenden Fenster können Sie angeben, welche Parameter bei der Wiederherstellung der empfohlenen Sicherheitsstufe beibehalten werden und für welche Komponenten diese gelten sollen.

Die Liste enthält die Programmkomponenten, deren Parameter vom Benutzer verändert wurden. Wenn für eine bestimmte Komponente bei der Arbeit exklusive Parameter festgelegt wurden, werden diese ebenfalls in der Liste angegeben.

Zu den exklusiven Parametern zählen die für die Anwendungskomponenten erstellten Ausnahmeregeln; die von Web-Anti-Virus verwendeten Listen der vertrauenswürdigen Internetadressen sowie die vom Proaktiven Schutz verwendeten Regeln für Anwendungen.

Diese Listen werden während der Arbeit des Programms erstellt. Da ihnen individuelle Aufgaben und Sicherheitsanforderungen zugrunde liegen, kann das Erstellen dieser Listen sehr zeitaufwändig sein. Deshalb wird empfohlen, sie beim Wiederherstellen der ursprünglichen Programmeinstellungen beizubehalten.

In der Grundeinstellung werden alle in der Liste enthaltenen Parameter gespeichert (die entsprechenden Kontrollkästchen sind deaktiviert). Wenn bestimmte Parameter nicht beibehalten werden sollen, aktivieren Sie die entsprechenden Kontrollkästchen.

Klicken Sie zum Abschluss der Konfiguration auf die Schaltfläche **Weiter**. Der Konfigurationsassistent wird gestartet (s. Pkt. 3.2 auf S. 35). Folgen Sie den Anweisungen.

Nach dem Abschluss des Assistenten wird für alle Schutzkomponenten die Sicherheitsstufe **Empfohlen** eingestellt, wobei die von Ihnen zum Speichern gewählten Parameter berücksichtigt werden. Zusätzlich werden die Einstellungen übernommen, die Sie während der Arbeit des Assistenten vorgenommen haben.

15.10. Technischer Support für Benutzer

Informationen über den technischen Support, den Kaspersky Lab seinen Benutzern anbietet, befinden sich im Abschnitt **Support** im Programmhauptfenster (s. Abb. 76).

Im oberen Bereich finden Sie allgemeine Informationen zur Anwendung: Anwendungsversion, Erscheinungsdatum der verwendeten Programm-

Datenbanken, sowie Angaben über das auf Ihrem Computer installierte Betriebssystem.

Wenn bei der Verwendung von Kaspersky Anti-Virus Probleme aufgetreten sind, prüfen Sie bitte zuerst, ob das vorliegende Hilfesystem oder die Wissensdatenbank auf der Webseite des Technischen Support-Services von Kaspersky Lab keine Lösungsmethode für Ihr Problem enthalten. Die Wissensdatenbank ist ein Abschnitt der Webseite des Technischen Support-Services und enthält Tipps über die Arbeit den Kaspersky-Lab-Produkten und Antworten auf häufige Fragen. Versuchen Sie, auf dieser Ressource eine Antwort auf Ihre Frage oder eine Lösung für Ihr Problem zu finden. Verwenden Sie den Link Technischer Online-Support, um zur Wissensdatenbank zu gelangen.

Eine weitere Ressource, die Informationen über die Arbeit mit der Anwendung bietet, ist das Benutzerforum für Kaspersky-Lab-Produkte. Diese Ressource ist ebenfalls ein Abschnitt der Webseite des Technischen Support Services und enthält Fragen, Kommentare und Vorschläge von Programmbenutzern. Sie können die wichtigsten Themen des Forums kennen lernen, eigene Beiträge über die Anwendung schreiben oder Antworten auf Ihre Frage suchen. Um zu dieser Ressource zu gehen, verwenden Sie den Link Benutzerforum.

Wenn Sie im Hilfesystem, in der Wissensdatenbank oder im Benutzerforum keine Lösung für Ihr Problem finden können, empfehlen wir Ihnen, sich an den Technischen Support-Service von Kaspersky Lab zu wenden.

Hinweis

Bitte beachten Sie, dass Sie als Benutzer einer kommerziellen Version von Kaspersky Anti-Virus registriert sein müssen, um den technischen Support in Anspruch zu nehmen. Die Benutzer von Testversionen der Anwendung besitzen keinen Anspruch auf technischen Support.

Die Registrierung erfolgt über den Aktivierungsassistenten der Anwendung (s. Pkt. 3.2.2 auf S. 36), wenn Sie die Anwendung mit Hilfe eines Aktivierungscodes aktivieren. In diesem Fall erhalten Sie zum Abschluss der Registrierung eine Kundennummer, die im Abschnitt **Support** (s. Abb. 76) des Programmhauptfensters angezeigt wird. Die Kundennummer ist die persönliche Identifikationsnummer des Benutzers, die eine obligatorische Bedingung für die Inanspruchnahme des technischen Supports per Telefon oder über das Webforum darstellt.

Wenn Sie die Anwendung mit Hilfe einer Schlüsseldatei aktivieren, können Sie sich direkt auf der Webseite des Technischen Support-Services registrieren.

Der neue Dienst Personal Cabinet bietet dem Benutzer Zugriff auf seinen persönlichen Bereich auf der Webseite des Technischen Support-Services. Im Personal Cabinet können Sie:

- eine Anfrage an den technischen Support schicken, ohne zuvor Anmeldedaten einzugeben.
- ohne Verwendung von E-Mails mit dem technischen Support korrespondieren.
- den Status Ihrer Anfragen in Echtzeit verfolgen.
- den vollständigen Verlauf Ihrer Anfragen an den technischen Support ansehen.
- eine Sicherungskopie Ihrer Schlüsseldatei erhalten.

Um über das Webforum Kontakt zum Technischen Support-Service aufzunehmen, verwenden Sie den Link Anfrage erstellen. Gehen Sie auf der automatisch geöffneten Webseite des Technischen Support-Services in Ihr Personal Cabinet und füllen Sie das Anfrageformular aus.

Zur Lösung dringender Probleme können Sie die im Hilfesystem genannten Servicenummern anrufen (s. Anhang B.2 auf S. 272). Der telefonische Support erfolgt rund um die Uhr und wird auf Russisch, Englisch, Französisch, Deutsch und Spanisch geleistet.

Um Informationen zu Kursen über Kaspersky-Lab-Produkte zu erhalten, verwenden Sie den Link Online-Kurse.

Support
Unsere Experten beantworten alle Fragen zu schädlichen Programmen und sonstigen Bedrohungen sowie zu Desinfektionsmethoden und Präventivmaßnahmen.
Informationen zum Programm
Anwendungsversion: 7.0.1.250
Erscheinungsdatum der Datenbanken 10/19/2007 3:23:10 PM
Betriebssystem Microsoft Windows XP Professional Service Pack 2 (build 2600)
Technischer Online-Support
Zur Wissensdatenbank des Technischen Support-Services von Kaspersky Lab gehen.
Benutzerforum
Personal Cabinet
Hier können Sie auf die Website Ihres "Personal Cabinet" gehen.
Anfrage erstellen | Online-Kurse

Abbildung 76. Informationen zum technischen Support

15.11. Arbeit mit der Anwendung beenden

Wenn es aus einem bestimmten Grund erforderlich ist, die Arbeit von Kaspersky Anti-Virus vollständig zu beenden, wählen Sie den Punkt **Beenden** im Kontextmenü (s. Pkt. 4.2 auf S. 46) des Programms. Dadurch wird das Programm aus dem Arbeitsspeicher entfernt, was bedeutet, dass Ihr Computer dann ungeschützt ist.

Wenn im Augenblick, als die Arbeit des Programms beendet wurde, auf dem Computer Netzwerkverbindungen vorhanden waren, die vom Programm kontrolliert wurden, dann erscheint auf dem Bildschirm eine Meldung darüber, dass diese Verbindungen getrennt wurden. Das ist eine Voraussetzung für das korrekte Beenden des Programms. Die Verbindungen werden automatisch nach 10 Sekunden oder durch Klick auf die Schaltfläche **Ja** getrennt. Die Mehrzahl der

getrennten Verbindungen wird nach einem bestimmten Zeitraum wiederhergestellt.

Hinweis

Wenn Sie während der Verbindungstrennung eine Datei herunterladen und dabei keinen Download-Manager verwenden, wird die Datenübertragung abgebrochen. Um die Datei herunterzuladen, müssen Sie den Download erneut initiieren.

Sie können das Trennen der Verbindungen ablehnen. Klicken Sie dazu im Meldungsfenster auf die Schaltfläche **Nein**. Dabei setzt das Programm seine Arbeit fort.

Nachdem Sie die Arbeit des Programms beendet haben, kann der Schutz des Computers erneut aktiviert werden, indem das Programm Kaspersky Anti-Virus über das Menü **Start → Programme → Kaspersky Anti-Virus 7.0 → Kaspersky Anti-Virus 7.0** gestartet wird.

Außerdem kann der Schutz nach dem Neustart des Betriebssystems automatisch gestartet werden. Um diesen Modus zu wählen, verwenden Sie im Konfigurationsfenster des Programms den Abschnitt **Service** (s. Abb. 72) und aktivieren Sie das Kontrollkästchen ☑ **Programm beim Hochfahren des Computers starten**.

KAPITEL 16. ARBEIT MIT DEM PROGRAMM AUS DER BEFEHLSZEILE

Sie können mit Kaspersky Anti-Virus mit Hilfe der Befehlszeile arbeiten. Dabei ist die Möglichkeit zum Ausführen der folgenden Operationen vorgesehen:

- Starten, Beenden, Anhalten und Fortsetzen der Arbeit von Komponenten der Anwendung.
- Starten, Beenden, Anhalten und Fortsetzen der Arbeit von Aufgaben zur Virensuche.
- Erhalt von Informationen über den aktuellen Status von Komponenten und Aufgaben sowie ihrer Statistik.
- Untersuchung von ausgewählten Objekten.
- Update der Datenbanken und Programm-Module.
- Aufruf der Hilfe über die Syntax der Befehlszeile.
- Aufruf der Hilfe über die Syntax eines Befehls.

Syntax der Befehlszeile:

```
avp.com <Befehl> [Parameter]
```

Hinweis

Der Zugriff auf die Anwendung über die Befehlszeile muss aus dem Installationsordner des Produkts oder unter Angabe des vollständigen Pfads von avp.com erfolgen.

Als **<Befehl>** werden verwendet:

ACTIVATE	Aktivierung der Anwendung über das Internet mit Hilfe eines Aktivierungscodes
ADDKEY	Aktivierung der Anwendung mit Hilfe einer Schlüsseldatei (dieser Befehl kann nur ausgeführt werden, wenn das über die Programmoberfläche festgelegte Kennwort angegeben wird)

START	Starten einer Komponente oder Aufgabe
PAUSE	Anhalten der Arbeit einer Komponente oder Aufgabe (dieser Befehl kann nur ausgeführt werden, wenn das über die Programmoberfläche festgelegte Kennwort angegeben wird)
RESUME	Fortsetzen der Arbeit einer Komponente oder Aufgabe
STOP	Beenden der Arbeit einer Komponente oder Aufgabe (dieser Befehl kann nur ausgeführt werden, wenn das über die Programmoberfläche festgelegte Kennwort angegeben wird)
STATUS	Bildschirmanzeige des aktuellen Status einer Komponente oder Aufgabe
STATISTICS	Bildschirmanzeige der Statistik über die Arbeit einer Komponente oder Aufgabe
HELP	Hilfe über die Befehlssyntax, Anzeige einer Befehlsliste
SCAN	Untersuchung von Objekten auf das Vorhandensein von Viren
UPDATE	Starten des Programm-Updates
ROLLBACK	Rückgängigmachen des letzten Updates der Anwendung (dieser Befehl kann nur ausgeführt werden, wenn das über die Programmoberfläche festgelegte Kennwort angegeben wird)
EXIT	Beenden der Arbeit mit dem Programm (dieser Befehl kann nur ausgeführt werden, wenn das über die Programmoberfläche festgelegte Kennwort angegeben wird)
IMPORT	Importieren von Schutzeinstellungen für die Anwendung (dieser Befehl kann nur ausgeführt werden, wenn das über die Programmoberfläche festgelegte Kennwort angegeben wird)

EXPORT	Exportieren von Schutzeinstellungen für die Anwendung

Jedem Befehl entspricht eine eigene Auswahl von Parametern, die für eine konkrete Komponente von Kaspersky Anti-Virus spezifisch sind.

16.1. Aktivierung der Anwendung

Die Aktivierung der Anwendung kann auf zwei Arten erfolgen:

- über das Internet mit Hilfe eines Aktivierungscodes (Befehl ACTIVATE)
- mit Hilfe einer Schlüsseldatei (Befehl ADDKEY)

Befehlssyntax:

```
ACTIVATE <Aktivierungscode> /password=<Kennwort>
ADDKEY <Dateiname>
```

Beschreibung der Parameter:

<Aktivierungscode>	Aktivierungscode für die Anwendung, den Sie beim Erwerb des Produkts erhalten haben.
<Dateiname>	Name der Schlüsseldatei für die Anwendung (Endung **.key*).
<Kennwort>	Kennwort für Kaspersky Anti-Virus, das über die Benutzeroberfläche der Anwendung festgelegt wurde.

Achtung!

Beachten Sie, dass dieser Befehl nur ausgeführt wird, wenn das Kennwort angegeben wird.

Beispiel:

```
avp.com ACTIVATE 11AA1-11AAA-1AA11-1A111
avp.com ADDKEY 1AA111A1.key /password=<Kennwort>
```

16.2. Steuerung von Anwendungskomponenten und Aufgaben

Syntax der Befehlszeile:

```
avp.com <Befehl> <Profil|Aufgabenname>
[/R[A]:<Berichtsdatei>]
avp.com STOP|PAUSE < Profil|Aufgabenname >
/password=<Kennwort> [/R[A]:<Berichtsdatei>]
```

Beschreibung der Parameter:

<Befehl>	Die Steuerung der Komponenten und Aufgaben von Kaspersky Anti-Virus wird mit Hilfe der folgenden Befehle ausgeführt: **START** – Start einer Echtzeitschutz-Komponente oder einer Aufgabe. **STOP** – Beenden einer Echtzeitschutz-Komponente oder einer Aufgabe. **PAUSE** – Anhalten der Arbeit einer Echtzeitschutz-Komponente oder einer Aufgabe. **RESUME** – Fortsetzen der Arbeit einer Echtzeitschutz-Komponente oder einer Aufgabe. **STATUS** – Den aktuellen Status einer Echtzeitschutz-Komponente oder einer Aufgabe auf dem Bildschirm anzeigen. **STATISTICS** – Die Statistik über die Arbeit einer Echtzeitschutz-Komponente oder einer Aufgabe auf dem Bildschirm anzeigen. Beachten Sie, dass die Befehle PAUSE und STOP nur ausgeführt werden, wenn das Kennwort eingegeben wird.
<Profil|Aufgabenname>	Als Wert des Parameters **<Profil>** können eine beliebige Echtzeitschutz-Komponente der Anwendung, ein Modul, das zu den Komponenten gehört, eine erstellte Untersuchungs- oder Upda-

	te-Aufgabe angegeben werden (Die von der Anwendung standardmäßig verwendeten Werte werden in der folgenden Tabelle genannt). Als Wert für den Parameter **<Aufgabenname>** kann der Name einer beliebigen vom Benutzer erstellten Untersuchungs- oder Update-Aufgabe angegeben werden.
<Kennwort>	Kennwort für Kaspersky Anti-Virus, das über die Anwendungsoberfläche angegeben wurde.
/R[A]:<Berichtsdatei>	**R:<Berichtsdatei>** – nur wichtige Ereignisse im Bericht protokollieren. **/RA:<Berichtsdatei>** – alle Ereignisse im Bericht protokollieren. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt und alle Ereignisse werden angezeigt.

Für den Parameter **<Profil>** wird einer der folgenden Werte angegeben:

RTP	alle Schutzkomponenten Der Befehl `avp.com START RTP` startet alle Echtzeitschutz-Komponenten, wenn der Schutz vollständig deaktiviert (s. Pkt. 6.1.2 auf S. 65) oder vorübergehend angehalten war (s. Pkt. 6.1.1 auf S. 64). Außerdem startet dieser Befehl jede beliebige Komponente des Echtzeitschutzes, deren Arbeit über die grafische Anwendungsoberfläche oder mit dem Befehl `PAUSE` aus der Befehlzeile angehalten wurde. Wenn eine Komponente über die grafische Anwendungsoberfläche oder mit dem Befehl `STOP` aus der Befehlszeile beendet wurde, wird sie durch den Befehl `avp.com START RTP` nicht gestartet. Zum Starten der Komponente muss der Befehl `avp.com START <Profil>` ausgeführt werden, wobei als <Profil> der Wert für eine konkrete Schutzkomponente verwendet wird, beispielsweise

	`avp.com START FM`.
FM	Datei-Anti-Virus
EM	Mail-Anti-Virus
WM	Web-Anti-Virus Werte für die Subkomponenten von Web-Anti-Virus: **httpscan** – Untersuchung des http-Datenstroms **sc** – Untersuchung von Skripts
BM	Proaktiver Schutz Werte für die Subkomponenten des Proaktiven Schutzes: **pdm** – Aktivitätsanalyse für Anwendungen
UPDATER	Update
Rollback	Rollback des letzten Updates der Anwendung
SCAN_MY_COMPUTER	die Aufgabe "Arbeitsplatz"
SCAN_CRITICAL_AREAS	die Aufgabe *"Kritische Bereiche"*
SCAN_STARTUP	die Aufgabe "Autostart-Objekte"
SCAN_QUARANTINE	Aufgabe zur Untersuchung der Quarantäneobjekte
SCAN_ROOTKITS	Aufgabe zur Suche nach Rootkits

Hinweis

Die aus der Befehlszeile gestarteten Komponenten und Aufgaben werden mit den Parametern ausgeführt, die im Interface des Programms festgelegt wurden.

Beispiele:

Um Datei-Anti-Virus zu aktivieren, geben Sie in der Befehlszeile ein:

```
avp.com START FM
```

Um den aktuellen Status des Proaktiven Schutzes für Ihren Computer anzuzeigen, geben Sie in der Befehlszeile ein:

```
avp.com STATUS BM
```

Um die Aufgabe Arbeitsplatz zu beenden, geben Sie in der Befehlszeile ein:

```
avp.com STOP SCAN_MY_COMPUTER /password=<Kennwort>
```

16.3. Virenuntersuchung von Objekten

Die Befehlszeile zum Starten der Virenuntersuchung eines bestimmten Bereichs und zur Bearbeitung von schädlichen Objekten besitzt folgendes allgemeines Aussehen:

```
avp.com SCAN [<Untersuchungsobjekt>] [<Aktion>] [<Da-
teitypen>] [<Ausnahmen>] [<Konfigurationsdatei>]
[<Berichtsparameter>][<zusätzliche Parameter>]
```

Hinweis

Für die Untersuchung von Objekten können Sie auch die in Kaspersky Anti-Virus erstellten Aufgaben verwenden, indem Sie die erforderliche Befehlszeile benutzen (s. Pkt. 16.1 auf S. 235). Dabei wird die Aufgabe mit den Parametern ausgeführt, die im Interface des Produkts festgelegt wurden.

Beschreibung der Parameter.

<Untersuchungsobjekt> - Der Parameter gibt eine Liste der Objekte an, die auf das Vorhandensein von schädlichem Code untersucht werden sollen.

Der Parameter kann mehrere Werte aus der folgenden Liste enthalten. Die Werte werden durch Leerzeichen getrennt.

<files>	Liste mit den Pfaden der Dateien und/oder Ordner für die Untersuchung. Die Angabe des absoluten oder relativen Pfads ist zulässig. Als Trennzeichen für die Elemente der Liste dient das Leerzeichen. Kommentare: • Wenn der Objektname ein Leerzeichen enthält, wird er in Anführungszeichen gesetzt. • Wenn ein konkreter Ordner angegeben wird, werden alle darin enthaltenen Dateien untersucht.
/MEMORY	Objekte des Arbeitsspeichers.
/STARTUP	Autostart-Objekte.
/MAIL	Mailboxen.
/REMDRIVES	alle Wechseldatenträger.
/FIXDRIVES	alle lokalen Laufwerke.
/NETDRIVES	alle Netzwerklaufwerke.
/QUARANTINE	Objekte in Quarantäne.
/ALL	vollständige Untersuchung des Computers.
/@:<filelist.lst>	Pfad der Datei mit einer Liste der Objekte und Ordner, die untersucht werden sollen. Die Datei muss das Textformat besitzen. Jedes Untersuchungsobjekt muss in einer separaten Zeile stehen. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Pfad ein Leerzeichen enthält, wird er in Anführungszeichen gesetzt.

<Aktion> - Der Parameter bestimmt die Aktionen mit einem schädlichen Objekt, das während der Untersuchung gefunden wird. Wenn der Parameter nicht angegeben wird, wird standardmäßig die Aktion ausgeführt, die dem Wert **/i8** entspricht.	
/i0	Keine Aktion ausführen, nur Informationen im Bericht protokollieren.
/i1	infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – überspringen.
/i2	infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – löschen; infizierte Objekte aus Containern (zusammengesetzten Objekten) nicht löschen; Container mit ausführbarer Kopfzeile (sfx-Archive) löschen (diese Aktion wird standardmäßig verwendet).
/i3	infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – löschen; Container-Objekte vollständig löschen, wenn die darin enthaltenen infizierten Dateien nicht gelöscht werden können.
/i4	infizierte Objekte löschen; Container-Objekte vollständig löschen, wenn die darin enthaltenen infizierten Dateien nicht gelöscht werden können.
/i8	den Benutzer beim Fund eines infizierten Objekts nach einer Aktion fragen
/i9	den Benutzer nach dem Abschluss der Untersuchung nach einer Aktion fragen
<Dateitypen> - Der Parameter bestimmt die Typen der Dateien, die der Virenuntersuchung unterzogen werden. Wenn der Parameter nicht angegeben wird, werden standardmäßig nur infizierbare Dateien nach ihrem Inhalt untersucht.	
/fe	nur infizierbare Dateien nach Erweiterung untersuchen.
/fi	nur infizierbare Dateien nach Inhalt untersuchen.

/fa	Alle Dateien untersuchen.
<Ausnahmen> - Der Parameter bestimmt die Objekte, die von der Untersuchung ausgeschlossen werden sollen. Der Parameter kann mehrere Werte aus der folgenden Liste enthalten. Die Werte werden durch Leerzeichen getrennt.	
-/e:a	Archive nicht untersuchen.
-/e:b	Mailboxen nicht untersuchen.
-/e:m	E-Mail-Nachrichten im Format plain text nicht untersuchen.
-e:<filemask>	Objekte nach Maske nicht untersuchen.
-e:<seconds>	Objekte überspringen, deren Untersuchung länger dauert, als der durch den Parameter **<seconds>** angegebene Zeitraum.
-es:<size>	Objekte überspringen, deren Größe (in MB) über dem Wert liegt, der durch den Parameter **<size>** bestimmt wird.
<Konfigurationsdatei> - bestimmt den Pfad der Konfigurationsfenster, in der die Parameter für die Arbeit des Programms bei der Untersuchung enthalten sind. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Werte verwendet, die im Interface von Kaspersky Anti-Virus festgelegt wurden.	
/C:<Dateiname>	Die Werte der Parameter, die in der Datei **<Dateiname>** angegeben sind, verwenden.
<Berichtsparameter> - Der Parameter bestimmt das Format des Berichts über die Untersuchungsergebnisse. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt. Alle Ereignisse werden angezeigt.	

/R:<Berichtsdatei>	nur wichtige Ereignisse in der angegebenen Berichtsdatei protokollieren.
/RA:<Berichtsdatei>	alle wichtigen Ereignisse in der angegebenen Berichtsdatei protokollieren.
<zusätzliche Parameter> – Parameter, der die Verwendung von Technologien zur Virenuntersuchung festlegt.	
/iChecker=<on|off>	Verwendung der Technologie iChecker aktivieren/deaktivieren.
/iSwift=<on|off>	Verwendung der Technologie iSwift aktivieren/deaktivieren.

Beispiele:

Untersuchung des Arbeitsspeichers, der Autostart-Objekte, der Mailboxen sowie der Ordner **My Documents**, **Program Files** *und der Datei* **test.exe***:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and
Settings\All Users\My Documents" "C:\Program Files"
"C:\Downloads\test.exe"
```

Anhalten der Untersuchung von ausgewählten Objekten, Starten der vollständigen Untersuchung des Computers, bei Abschluss der Untersuchung soll die Virensuche in den ausgewählten Objekten fortgesetzt werden:

```
avp.com PAUSE SCAN_OBJECTS /password=<Kennwort>
avp.com START SCAN_MY_COMPUTER
avp.com RESUME SCAN_OBJECTS
```

Untersuchung der Objekte, deren Liste in der Datei ***object2scan.txt*** *angegeben ist. Für die Arbeit soll die Konfigurationsdatei* ***scan_setting.txt*** *verwendet werden. Über die Untersuchungsergebnisse soll ein Bericht erstellt werden, in dem alle Ereignisse aufgezeichnet werden:*

```
avp.com SCAN /MEMORY /@:objects2scan.txt
/C:scan_settings.txt /RA:scan.log
```

Beispiel für die Konfigurationsdatei:

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt
/RA:scan.log
```

16.4. Programm-Update

Der Befehl für das Update der Programm-Datenbanken und Module für Kaspersky Anti-Virus besitzt folgende Syntax:

```
avp.com UPDATE [<Updatequelle>]
[/R[A]:<Berichtsdatei>] [/C:<Dateiname>]
[/APP=<on|off>]
```

Beschreibung der Parameter:

<Updatequelle>	HTTP-, FTP-Server oder Netzwerkordner für den Download der Updates. Als Wert für diesen Parameter kann der vollständige Pfad oder die URL-Adresse der Updatequelle angegeben werden. Wenn der Pfad nicht angegeben wird, wird die Updatequelle aus den Einstellungen des Diensts für das Programm-Update übernommen.
/R[A]:<Berichtsdatei>	**/R:<Berichtsdatei>** - nur wichtige Ereignisse im Bericht protokollieren. **/RA:<Berichtsdatei>** - alle Ereignisse im Bericht protokollieren. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt. Alle Ereignisse werden angezeigt.
/C:<Dateiname>	Pfad der Konfigurationsdatei, die die Parameter für die Arbeit des Programms beim Update enthält. Die Angabe des absoluten oder relativen Pfads ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Werte verwendet, die im Interface von Kaspersky Anti-Virus festgelegt wurden.
/APP=<on|off>	Update der Programm-Module aktivieren/deaktivieren.

Beispiele:

Update der Bedrohungssignaturen, alle Ereignisse protokollieren:

```
avp.com UPDATE /RA:avbases_upd.txt
```

*Update der Datenbanken für Kaspersky Anti-Virus, die Parameter der Konfigurationsdatei **updateapp.ini** verwenden:*

```
avp.com UPDATE /APP=on /C:updateapp.ini
```

Beispiel für die Konfigurationsdatei:

```
"ftp://my_server/kav updates" /RA:avbases_upd.txt
/app=on
```

16.5. Rollback des letzten Updates der Anwendung

Syntax der Befehlszeile:

```
ROLLBACK [/R[A]:<Berichtsdatei>] [/password=<Kennwort>]
```

/R[A]:<Berichtsdatei>	**/R:<Berichtsdatei>** - nur wichtige Ereignisse im Bericht festhalten. **/RA:<Berichtsdatei>** - alle Ereignisse im Bericht festhalten. Es kann der absolute oder relative Pfad der Datei angegeben werden. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.
<Kennwort>	Kennwort für Kaspersky Anti-Virus, das über die Programmoberfläche festgelegt wurde.

Achtung!

Beachten Sie, dass dieser Befehl nur ausgeführt wird, wenn das Kennwort angegeben wird.

Beispiel:

```
avp.com ROLLBACK /RA:rollback.txt /password=<Kennwort>
```

16.6. Export von Schutzparametern

Syntax der Befehlszeile:

```
avp.com EXPORT <Profil> <Dateiname>
```

Beschreibung der Parameter:

<Profil>	Komponente oder Aufgabe, für die der Export von Parametern ausgeführt wird. Als Wert des Parameters **<Profil>** kann einer der in Pkt. 16.2 auf S. 236 genannten Werte verwendet werden.
<Dateiname>	Pfad der Datei, in welche die Parameter von Kaspersky Anti-Virus exportiert werden. Ein absoluter oder relativer Pfad kann angegeben werden. Die Konfigurationsdatei wird im Binärformat (dat) gespeichert und kann später zum Übertragen von Anwendungseinstellungen auf andere Computer verwendet werden. Die Konfigurationsdatei kann auch im Textformat gespeichert werden. Dazu erhält der Dateiname die Endung *txt*. Diese Datei kann nur zur Ansicht der grundlegenden Funktionsparameter der Anwendung verwendet werden.

Beispiele:

```
avp.com EXPORT c:\settings.dat
```

16.7. Import von Schutzparametern

Syntax der Befehlszeile:

```
avp.com IMPORT <Dateiname> [/password=<Kennwort>]
```

<Dateiname>	Pfad der Datei, aus welcher die Parameter von Kaspersky Anti-Virus importiert werden. Ein absoluter oder relativer Pfad kann angegeben werden.

<Kennwort>	Kennwort für Kaspersky Anti-Virus, das über die Programmoberfläche festgelegt wurde.

Achtung!

Beachten Sie, dass dieser Befehl nur ausgeführt wird, wenn das Kennwort angegeben wird.

Beispiel:

```
avp.com IMPORT c:\settings.dat /password=<Kennwort>
```

16.8. Anwendung starten

Syntax der Befehlszeile:

```
avp.com
```

16.9. Anwendung beenden

Syntax der Befehlszeile:

```
EXIT /password=<Kennwort>
```

<Kennwort>	Kennwort für Kaspersky Anti-Virus, das über die Programmoberfläche festgelegt wurde.

Achtung!

Beachten Sie, dass dieser Befehl nur ausgeführt wird, wenn das Kennwort angegeben wird.

Beachten Sie, dass dieser Befehl nur ausgeführt wird, wenn das Kennwort angegeben wird.

16.10. Anlegen einer Tracing-Datei

Das Anlegen einer Tracing-Datei kann erforderlich sein, wenn bei der Arbeit mit der Anwendung Probleme auftreten, deren genaue Analyse durch die Experten des Technischen Support-Services notwendig ist.

Befehlssyntax:

```
avp.com TRACE [file] [on|off] [<Tracing-Niveau>]
```

[on|off]	Anlegen der Tracing-Datei aktivieren/deaktivieren.
[file]	Tracing in Form einer Datei erstellen.
<Tracing-Niveau>	Für diesen Parameter kann ein Zahlenwert im Bereich von 0 (minimale Stufe, nur kritische Meldungen) bis 700 (maximale Stufe, alle Meldungen) festgelegt werden. Wenn Sie sich an den Technischen Support-Service wenden, nennt Ihnen der zuständige Spezialist das erforderliche Tracing-Niveau. Andernfalls gilt das Niveau 500 als empfehlenswert.

Achtung!

Es wird empfohlen, das Anlegen von Tracing-Dateien nur zur Diagnose eines konkreten Problems zu aktivieren. Sollte das Tracing ständig aktiv sein, so kann die Leistungsfähigkeit des Computers sinken und es kann zu einer Überfüllung der Festplatte kommen.

Beispiele:

Erstellen von Tracing-Dateien deaktivieren:

```
avp.com TRACE file off
```

Erstellen einer Tracing-Datei zum Senden an den Technischen Support-Service, mit einem maximalen Tracing-Niveau von 500:

```
avp.com TRACE file on 500
```

16.11. Anzeige der Hilfe

Zur Anzeige der Hilfe über die Syntax der Befehlzeile dient folgender Befehl:

```
avp.com [ /? | HELP ]
```

Um Hilfe über die Syntax eines konkreten Befehls zu erhalten, können Sie einen der folgenden Befehle verwenden:

```
avp.com <Befehl> /?
avp.com HELP <Befehl>
```

16.12. Rückgabecodes der Befehlszeile

In diesem Abschnitt werden die Rückgabecodes der Befehlszeile beschrieben. Die allgemeinen Codes können von einem beliebigen Befehl der Befehlszeile zurückgegeben werden. Als Rückgabecodes für Aufgaben sind die allgemeinen Codes sowie spezifische Codes für einen konkreten Aufgabentyp möglich.

Allgemeine Rückgabecodes	
0	Operation wurde erfolgreich ausgeführt
1	Ungültiger Parameterwert
2	Unbekannter Fehler
3	Fehler bei der Aufgabenausführung
4	Aufgabenausführung wurde abgebrochen
Rückgabecodes für Aufgaben zur Virensuche	
101	Alle gefährlichen Objekte wurden bearbeitet
102	Es wurden gefährliche Objekte gefunden

KAPITEL 17. PROGRAMM ÄNDERN, REPARIEREN ODER LÖSCHEN

Das Programm kann auf zwei Arten deinstalliert werden:

- mit Hilfe des Installationsassistenten der Anwendung (s. Pkt. 17.1 auf S. 250);
- aus der Befehlszeile (s. Pkt. 17.2 auf S. 252).

17.1. Ändern, Reparieren oder Löschen des Programms mit Hilfe des Installationsassistenten

Die Reparatur des Programms kann dann von Nutzen sein, wenn Sie Fehler in seiner Arbeit feststellen, die auf inkorrekte Einstellungen oder beschädigte Programmdateien zurückgehen.

Das Ändern des Komponentenbestands erlaubt Ihnen, bestimmte Komponenten von Kaspersky Anti-Virus nachträglich zu installieren oder jene Komponenten zu löschen, die Sie bei der Arbeit stören oder nicht gebraucht werden.

Um den ursprünglichen Programmzustand wiederherzustellen, um Komponenten von Kaspersky Anti-Virus, die bei der Erstinstallation nicht installiert wurden, zu installieren, oder um das Programm zu löschen,

1. Legen Sie die CD/DVD mit der Programmdistribution in das CD/DVD-ROM-Laufwerk ein, wenn die Installation von dort aus erfolgte. Wenn die Installation von Kaspersky Anti-Virus aus einer anderen Quelle erfolgte (gemeinsamer Ordner, Ordner auf der Festplatte usw.), vergewissern Sie sich, dass die Programmdistribution in dieser Quelle vorhanden ist und Sie zum Zugriff berechtigt sind.
2. Wählen Sie **Start → Programme → Kaspersky Anti-Virus 7.0 → Ändern, Reparieren oder Löschen**.

Dadurch wird das Installationsprogramm in Form eines Assistenten gestartet. Im Folgenden werden die Schritte zur Reparatur, zum Ändern des Bestands der Programmkomponenten und zum Löschen des Programms ausführlich beschrieben.

Schritt 1. Auswahl einer Operation

Zuerst müssen Sie festlegen, welche Operation Sie mit dem Programm vornehmen möchten: Zur Auswahl stehen das Ändern der Programmkomponenten, das Wiederherstellen des ursprünglichen Zustands der installierten Komponenten oder das Löschen bestimmter Komponenten oder des ganzen Programms. Klicken Sie zum Ausführen der von Ihnen gewünschten Operation auf die entsprechende Schaltfläche. Die weitere Aktion des Installationsprogramms ist von der gewählten Operation abhängig.

Das Ändern des Komponentenbestands entspricht der benutzerdefinierten Installation des Programms (s. Schritt 6. auf S. 33), bei der Sie festlegen können, welche Komponenten installiert und welche gelöscht werden sollen.

Die Reparatur des Programms erfolgt auf Basis der installierten Komponenten. Alle Dateien der Komponenten, die installiert sind, werden aktualisiert und für jede dieser Komponenten wird die empfohlene Sicherheitsstufe eingestellt.

Beim Löschen des Programms können Sie wählen, welche der bei der Arbeit des Programms erstellten und verwendeten Daten, auf Ihrem Computer gespeichert werden sollen. Um alle Daten von Kaspersky Anti-Virus zu löschen, wählen Sie die Variante **Die Anwendung vollständig löschen**. Um bestimmte Daten zu speichern, wählen Sie die Variante **Objekte der Anwendung speichern** und geben Sie an, welche Objekte beibehalten werden sollen:

- *Aktivierungsdaten* – Schlüsseldatei für das Programm.
- *Programm-Datenbanken* – vollständige Signaturen der gefährlichen Programme, Viren und anderen Bedrohungen, die beim letzten Update aktuell waren.
- *Backup-Objekte* – Sicherungskopien von gelöschten oder desinfizierten Objekten. Es wird empfohlen, diese Objekte zu speichern, um sie bei Bedarf später wiederherzustellen.
- *Quarantäneobjekte* – Objekte, die möglicherweise von Viren oder Virusmodifikationen infiziert sind. Solche Objekte enthalten Code, der Ähnlichkeit mit dem Code eines bekannten Virus besitzt. Allerdings lässt sich nicht sicher sagen, ob sie schädlich sind. Es wird empfohlen, diese Objekte zu speichern, weil sie sich als virenfrei erweisen oder später unter Verwendung von aktualisierten Programm-Datenbanken desinfiziert werden können.

- *Schutzeinstellungen* – Parameterwerte für die Arbeit aller Programmkomponenten.
- *iSwift-Daten* – Datenbank, die Informationen über untersuchte Objekte des NTFS-Dateisystems enthält. Sie erlaubt die Beschleunigung der Untersuchung von Objekten. Durch die Verwendung dieser Datenbank untersucht Kaspersky Anti-Virus nur jene Objekte, die seit der letzten Untersuchung verändert wurden.

Achtung!

Wenn zwischen der Deinstallation einer Version von Kaspersky Anti-Virus und der Installation einer anderen Version ein größerer Zeitraum liegt, wird davon abgeraten, die aus der vorherigen Programminstallation stammende *iSwift*-Datenbank zu verwenden. In der Zwischenzeit kann ein gefährliches Programm auf den Computer gelangt sein, dessen schädliche Aktionen bei Verwendung dieser Datenbank nicht erkannt werden, was zu einer Infektion des Computers führen kann.

Klicken Sie auf die Schaltfläche **Weiter**, um die gewählte Operation zu starten. Der Prozess zum Kopieren der notwendigen Dateien auf Ihren Computer oder zum Löschen der ausgewählten Komponenten und Daten wird gestartet.

Schritt 2. Abschluss der Operation zum Reparieren, Ändern oder Löschen des Programms

Der Prozess zum Reparieren, Ändern oder Löschen wird auf dem Bildschirm dargestellt. Danach werden Sie über den Abschluss des Prozesses informiert.

Die Deinstallation macht in der Regel den Neustart des Computers erforderlich, weil Änderungen im System berücksichtigt werden müssen. Auf dem Bildschirm erscheint eine Bestätigungsabfrage für den Neustart des Computers. Klicken Sie auf die Schaltfläche **Ja**, um den Neustart sofort vorzunehmen, oder auf die Schaltfläche **Nein**, um den Computer später manuell neu zu starten.

17.2. Deinstallation des Programms aus der Befehlszeile

Um Kaspersky Anti-Virus aus der Befehlszeile zu deinstallieren, geben Sie ein:

```
msiexec /x <Paketname>
```

Es wird ein Installationsassistent gestartet (s. Kapitel 17 auf S. 250), mit dessen Hilfe Sie die Deinstallation der Anwendung vornehmen können.

Um die Anwendung im Silent-Modus ohne Neustart des Computers zu deinstallieren (der Neustart muss nach der Deinstallation manuell erfolgen), geben Sie folgende Befehlszeile ein:

```
msiexec /x <Paketname> /qn
```

KAPITEL 18. HÄUFIGE FRAGEN

In diesem Kapitel behandeln wir die von Benutzern am häufigsten gestellten Fragen zu Installation, Konfiguration und Arbeit mit Kaspersky Anti-Virus und versuchen, sie eingehend zu beantworten.

Frage: Kann Kaspersky Anti-Virus 7.0 mit Antiviren-Produkten anderer Hersteller genutzt werden?

Um Konflikte zu vermeiden, empfehlen wir, die Antiviren-Software anderer Hersteller vor der Installation von Kaspersky Anti-Virus zu deinstallieren.

Frage: Eine Datei wird von Kaspersky Anti-Virus nicht wiederholt untersucht. Warum?

In der Tat untersucht Kaspersky Anti-Virus eine Datei nicht doppelt, wenn sie seit der letzten Untersuchung nicht geändert worden ist.

Das wird durch die Verwendung der neuen Technologien iChecker™ und iSwift™ ermöglicht. Dabei wird eine Datenbank mit Kontrollsummen der Objekte verwendet und die Kontrollsummen von Dateien werden in zusätzlichen NTFS-Strömen gespeichert.

Frage: Wozu ist die Aktivierung der Anwendung erforderlich? Funktioniert Kaspersky Anti-Virus auch ohne Schlüsseldatei?

Kaspersky Anti-Virus kann ohne Schlüssel arbeiten. Allerdings stehen in diesem Fall das Programm-Update und die Unterstützung durch den Technischen Support-Service nicht zur Verfügung.

Wenn Sie sich noch nicht für den Kauf von Kaspersky Anti-Virus entschieden haben, können wir Ihnen einen Testschlüssel mit einer Gültigkeit von zwei Wochen oder einen Monat anbieten. Nach Ablauf der Testdauer wird der Schlüssel gesperrt.

Frage: Nach der Installation von Kaspersky Anti-Virus verhält sich das Betriebssystem ungewöhnlich ("Einfrieren auf blauem Bildschirm", wiederholter Neustart des Computers u.a.). Was tun?

Diese Situation tritt selten ein, kann aber durch einen Konflikt zwischen Kaspersky Anti-Virus und einem auf Ihrem Computer installierten Programm verursacht werden.

Gehen Sie folgendermaßen vor, um die Funktionsfähigkeit Ihres Betriebssystems wiederherzustellen:

1. Klicken Sie gleich nachdem der Computer gestartet wurde solange auf die Taste **F8**, bis das Auswahlmenü für die Startvarianten des Betriebssystems erscheint.
2. Wählen Sie den Punkt **Abgesicherter Modus** und laden Sie das Betriebssystem.
3. Starten Sie Kaspersky Anti-Virus.
4. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie den Abschnitt **Service**.
5. Deaktivieren Sie das Kontrollkästchen **Programm beim Hochfahren des Computers starten** und klicken Sie auf die Schaltfläche **OK**.
6. Starten Sie das Betriebssystem im gewöhnlichen Modus neu.

Senden Sie eine Anfrage an den Technischen Support-Service von Kaspersky Lab. Öffnen Sie dazu das Programmhauptfenster, wählen Sie den Abschnitt **Support** und verwenden Sie den Link Anfrage erstellen. Beschreiben Sie das Problem und die entsprechenden Bedingungen möglichst genau..

Fügen Sie Ihrer Anfrage unbedingt eine Datei mit dem vollständigen Speicherabbild des Betriebssystem Microsoft Windows bei. Diese Datei wird folgendermaßen erstellt:

1. Klicken Sie mit der rechten Maustaste auf das Symbol **Arbeitsplatz** und wählen Sie im folgenden Fenster den Punkt **Eigenschaften**.
2. Wählen Sie im folgenden Fenster **Systemeigenschaften** die Registerkarte **Erweitert** und klicken Sie im Abschnitt **Starten und Wiederherstellen** auf die Schaltfläche **Einstellungen**.
3. Wählen Sie im Fenster **Starten und Wiederherstellen** im Abschnitt **Debuginformationen speichern** aus der Dropdown-Liste den Wert **Vollständiges Speicherabbild**.

   Die Datei mit dem Speicherabbild wird standardmäßig unter dem Namen *memory.dmp* im Systemverzeichnis gespeichert. Sie können einen anderen Ordner zum Speichern des Dumps festlegen. Ändern Sie dazu im entsprechenden Feld den Ordnernamen.
4. Wiederholen Sie den Vorgang, bei dem das mit der Arbeit von Kaspersky Anti-Virus verbundene Problem aufgetreten ist.
5. Vergewissern Sie sich, dass die Datei mit dem vollständigen Speicherabbild erfolgreich gespeichert wurde.

ANHANG A. ZUSÄTZLICHE INFORMATIONEN

Dieser Anhang enthält Informationen über die Formate von zu untersuchenden Dateien und über zulässige Masken, die bei der Konfiguration von Kaspersky Anti-Virus verwendet werden können.

A.1. Liste der Objekte, die nach Erweiterung untersucht werden

Wenn Sie als Untersuchungsobjekte für Datei-Anti-Virus oder für eine Untersuchungsaufgabe die Variante **Programme und Dokumente (nach Erweiterung) untersuchen** gewählt haben, dann werden Dateien mit den unten aufgezählten Erweiterungen ausführlich auf Viren analysiert. Die gleichen Dateien werden auch von Mail-Anti-Virus untersucht, wenn die Filterung von Objekten aktiviert ist, die an E-Mails angehängt sind:

com – ausführbare Programmdatei.

exe – ausführbare Datei, selbstextrahierendes Archiv.

sys – Systemtreiber.

prg – Text der Programme dBase, Clipper oder Microsoft Visual FoxPro, Programm des Pakets WAVmaker.

bin – Binärdatei.

bat – Datei einer Paketaufgabe.

cmd – Befehlsdatei für Microsoft Windows NT (entspricht einer bat-Datei für DOS), OS/2.

dpl – komprimierte Bibliothek für Borland Delphi.

dll – Dynamic Link Library (Dynamische Verbindungsbibliothek).

scr – Bildschirmschonerdatei für Microsoft Windows.

cpl – Systemsteuerungsmodul (control panel) in Microsoft Windows.

ocx – Microsoft OLE-Objekt (Object Linking and Embedding).

tsp – Programm, das im Timesharing-Modus arbeitet.

drv – Treiber für ein bestimmtes Gerät.

vxd – Treiber für ein virtuelles Microsoft-Windows-Gerät.

pif – Datei mit Informationen zum Programm.

lnk – Linkdatei in Microsoft Windows.

reg – Registrierungsdatei für Schlüssel der Microsoft Windows-Systemregistrierung.

ini – Initialisierungsdatei.

cla – Java-Klasse.

vbs – Visual-Basic-Skript.

vbe – BIOS-Video-Erweiterung.

js, jse – JavaScript-Quelltext.

htm – Hypertext-Dokument.

htt – Hypertext-Entwicklung von Microsoft Windows.

hta – Hypertext-Programm für Microsoft Internet Explorer.

asp – Active-Server-Pages-Skript.

chm – kompilierte HTML-Datei.

pht – HTML-Datei mit eingebettetem PHP-Skript.

php – Skript, das in eine HTML-Datei eingebettet wird.

wsh – Microsoft Windows Script Host-Datei.

wsf – Microsoft-Windows-Skript.

the – Bildschirmschonerdatei für den Arbeitsplatz von Microsoft Windows 95

hlp – Hilfedatei des Formats Win Help.

eml – E-Mail-Nachricht für Microsoft Outlook Express.

nws – neue E-Mail-Nachricht für Microsoft Outlook Express.

msg – E-Mail-Nachricht für Microsoft Mail.

plg – E-Mail-Nachricht

mbx – Erweiterung für eine gespeicherte Nachricht in Microsoft Office Outlook.

*doc** – Dokument für Microsoft Office Word, z.B.: *doc* – Dokument für Microsoft Office Word, *docx* – Dokument für Microsoft Office Word 2007 mit XML-Unterstützung, *docm* – Dokument für Microsoft Office Word 2007 mit Makro-Unterstützung.

*dot** – Dokumentvorlage für Microsoft Office Word, z.B.: *dot* – Dokumentvorlage für Microsoft Office Word, *dotx* – Dokumentvorlage für Microsoft Office Word 2007, *dotm* – Dokumentvorlage für Microsoft Office Word 2007 mit Makro-Unterstützung.

fpm – Datenbankprogramm, Startdatei für Microsoft Visual FoxPro.

rtf – Dokument im Rich-Text-Format.

shs – Fragment für Shell Scrap Object Handler.

dwg – Datenbank für AutoCAD-Skizzen.

msi – Microsoft Windows Installer-Paket.

otm – VBA-Projekt für Microsoft Office Outlook.

pdf – Adobe Acrobat-Dokument.

swf – Shockwave Flash-Paketobjekt.

jpg, jpeg, png – Grafikdatei zum Speichern von komprimierten Bildern.

emf – Datei des Formats Enhanced Metafile. Folgegeneration einer Metadatei des Betriebssystems Microsoft Windows. EMF-Dateien werden von 16-Bit -Microsoft Windows nicht unterstützt.

ico – Symboldatei für ein Objekt.

ov? – ausführbare Datei für MS DOS.

*xl** – Dokumente und Dateien für Microsoft Office Excel, z.B.: *xla* – Erweiterung für Microsoft Office Excel, *xlc* – Diagramm, *xlt* – Dokumentvorlage, *xlsx* – Arbeitsmappe für Microsoft Office Excel 2007, *xltm* – Arbeitsmappe für Microsoft Office Excel 2007 mit Makro-Unterstützung, *xlsb* – Arbeitsmappe für Microsoft Office Excel 2007 im Binärformat (nicht XML), *xltx* – Vorlage für Microsoft Office Excel 2007, *xlsm* – Vorlage für Microsoft Office Excel 2007 mit Makro-Unterstützung, *xlam* – Snap-In für Microsoft Office Excel 2007 mit Makro-Unterstützung.

*pp** – Dokumente und Dateien für Microsoft Office PowerPoint, z.B.: *pps* – Dia für Microsoft Office PowerPoint, *ppt* – Präsentation, *pptx* – Präsentation für Microsoft Office PowerPoint 2007, *pptm* – Präsentation für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung, *potx* – Präsentationsvorlage für Microsoft Office PowerPoint 2007, *potm* – Präsentationsvorlage für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung, *ppsx* – Diashow für Microsoft Office PowerPoint 2007, *ppsm* – Diashow für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung, *ppam* – Snap-In für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung.

*pp** – Dokumente und Dateien für Microsoft Office PowerPoint, z.B.: *pps* – Dia für Microsoft Office PowerPoint, *ppt* – Präsentation usw.

*md** – Dokumente und Dateien für Microsoft Office Access, z.B.: *mda* – Arbeitsgruppe für Microsoft Office Access, mdb – Datenbank usw.

sldx – Dia für Microsoft Office PowerPoint 2007.

sldm – Dia für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung.

thmx – Thema für Microsoft Office 2007.

Achtung!

Beachten Sie, dass das tatsächliche Format einer Datei von dem Format abweichen kann, das in der Dateierweiterung angegeben ist.

A.2. Zulässige Ausschlussmasken für Dateien

Hier werden Beispiele für zulässige Masken genannt, die Sie beim Erstellen der Liste auszuschließender Dateien verwenden können:

1. Masken ohne Dateipfad:
   - ***.exe** – alle Dateien mit der Endung *exe*
   - ***.ex?** – alle Dateien mit der Endung *ex?,* wobei anstelle von ? ein beliebiges Zeichen stehen kann.
   - **test** – alle Dateien mit dem Namen *test*
2. Masken mit absolutem Dateipfad:
   - **C:\dir*.*** oder **C:\dir*** oder **C:\dir** – alle Dateien im Ordner *C:\dir*
   - **C:\dir*.exe** – alle Dateien mit der Endung *exe* im Ordner *C:\dir*
   - **C:\dir*.ex?** – alle Dateien mit der Endung *ex?* im Ordner *C:\dir\,* wobei anstelle von ? ein beliebiges Zeichen stehen kann.
   - **C:\dir\test** – nur die Datei *C:\dir\test*

     Um zu verhindern, dass die Dateien in allen untergeordneten Ordnern des gewählten Ordners untersucht werden, aktivieren Sie beim Erstellen der Maske das Kontrollkästchen **Unterordner einschließen**.
3. Masken mit relativem Dateipfad:
   - **dir*.*** oder **dir*** oder **dir** – alle Dateien in allen Ordnern von *dir*
   - **dir\test** – alle Dateien *test* in den Ordnern von *dir*
   - **dir*.exe** – alle Dateien mit der Endung *exe* in allen Ordnern von *dir*
   - **dir*.ex?** – alle Dateien mit der Endung *ex?* in allen Ordnern von *dir\,* wobei anstelle von ? ein beliebiges Zeichen stehen kann.

     Um zu verhindern, dass die Dateien in allen untergeordneten Ordnern des gewählten Ordners untersucht werden, aktivieren Sie beim Erstellen der Maske das Kontrollkästchen **Unterordner einschließen**.

Hinweis

Die Verwendung der Ausnahmemasken ***.*** oder * ist nur unter Angabe des Typs der auszuschließenden Bedrohung entsprechend der Viren-Enzyklopädie zulässig. In diesem Fall wird die Bedrohung nicht in allen Objekten gefunden werden. Die Verwendung dieser Masken ohne Angabe eines Bedrohungstyps entspricht dem Deaktivieren des Echtzeitschutzes.

Außerdem wird davor gewarnt, als Ausnahme ein virtuelles Laufwerk zu wählen, das auf der Basis eines Ordners des Dateisystems mit dem Befehl *subst* erstellt wurde. Dies wäre sinnlos, da das Programm das virtuelle Laufwerk bei der Untersuchung als Ordner betrachten und folglich untersuchen würde.

A.3. Zulässige Ausschlussmasken nach der Klassifikation der Viren-Enzyklopädie

Wenn eine Bedrohung mit einem bestimmten Status nach der Klassifikation der Viren-Enzyklopädie als Ausnahme hinzugefügt wird, können Sie angeben:

- den vollständigen Namen der Bedrohung, wie er in der Viren-Enzyklopädie auf der Seite www.viruslist.com/de genannt wird (beispielsweise **not-a-virus:RiskWare.RemoteAdmin.RA.311** oder **Flooder.Win32.Fuxx**).
- den Namen der Bedrohung als Maske, beispielsweise:
  - **not-a-virus*** – legale, aber potentiell gefährliche Programme sowie Scherzprogramme von der Untersuchung ausschließen.
  - ***Riskware.*** – alle potentiell gefährlichen Programme des Typs Riskware von der Untersuchung ausschließen.
  - ***RemoteAdmin.*** – alle Programmversionen zur entfernten Verwaltung von der Untersuchung ausschließen.

ANHANG B. KASPERSKY LAB

Das Unternehmen

Kaspersky Lab ist ein weltweit führendes Unternehmen in den Bereichen Viren-, Spam- und Hacker-Schutz. Unser hoch spezialisiertes Viren-Labor reagiert stets schneller als alle anderen auf neue Bedrohungen, so dass unsere innovativen Programme seit vielen Jahren Heimanwender und Unternehmen jeder Größe zuverlässig schützen.

Bereits 1997 wurde Kaspersky Lab von dem russischen Virenexperten Eugene Kaspersky in Moskau gegründet und hat heute unter anderem Niederlassungen in Deutschland, Frankreich, Großbritannien, Polen, Japan, USA und China.

Einzigartige Erfahrung

Weltweit beschäftigt Kaspersky Lab über 550 hochspezialisierte Mitarbeiter, darunter Mitglieder der Computer Anti-Virus Researchers Organisation (CARO) und des Virus Bulletin Technical Advisory Board. Im Laufe vieler Jahre Forschung und Kampf gegen Computerviren haben wir Wissen und Fähigkeiten erworben, die heute unser wertvollstes Kapital darstellen.

Dank unserer weit reichenden Erfahrung sind wir in der Lage, Entwicklungstrends bei Malware vorherzusehen. Dieser einzigartige Vorteil bildet die Basis der Produkte und Dienstleistungen von Kaspersky Lab, so dass wir anderen immer einen Schritt voraus sind und unseren Kunden stets den besten Schutz bieten können.

Kaspersky Anti-Virus

Nach vielen Jahren innovativer Entwicklungen zählt Kaspersky Lab heute zu den führenden Herstellern von Sicherheits-Software. Der hohe Standard unserer Produkte wird durch zahlreiche Auszeichnungen internationaler Forschungseinrichtungen, unabhängiger Testlabors und renommierter Fachpublikationen bestätigt.

Die Programm-Module unseres bekanntesten Programms, Kaspersky Anti-Virus, gewährleisten einen zuverlässigen Schutz für Workstations, Datei- und Web-Server, Mail-Gateways, Firewalls, Pocket-PCs und Smartphones.

Als erstes Unternehmen entwickelte Kaspersky Lab bedeutende Technologien, die heute selbst bei zahlreichen Antiviren-Programmen anderer Hersteller – wie G-Data, Aladdin und F-Secure – als Programm-Kern einen unverzichtbaren Bestandteil bilden. So vertrauen bereits über 200 Millionen Anwender unseren Innovationen, wie dem heuristischen Analysator zur Entdeckung noch unbekannter Viren, den Micro-Updates für die Antiviren-Datenbanken und dem ersten umfassenden Virenschutz für Unix/Linux-Systeme.

Komplexe Technologien für Ihre Sicherheit

Moderne Viren und Schadprogramme sind komplexe Bedrohungen, so dass die bisher üblichen Schutzpakete für PCs und Netzwerke häufig nicht mehr ausreichen.

Aus diesem Grund entwickelte Kaspersky Lab mit Kaspersky Anti-Hacker eine Personal Firewall und mit Kaspersky Anti-Spam einen besonders effektiven Spam-Filter. Mit den Produkten von Kaspersky Lab können Sie Ihren Computer und Ihr Netzwerk optimal vor allen modernen virtuellen Gefahren schützen.

Service

Kaspersky Lab bietet seinen Kunden eine ganze Palette zusätzlicher Dienstleistungen, die einen maximalen Schutz garantieren: Die Antiviren-Datenbanken werden stündlich aktualisiert, die Anti-Spam-Dateien 12 bis 24 Mal pro Tag. Zudem steht allen Anwendern ein rund-um-die-Uhr-Support zur Verfügung: Telefonisch oder per E-Mail – in deutscher, englischer, russischer und französischer Sprache.

B.1. Weitere Produkte und Services von Kaspersky Lab

Kaspersky Lab News Agent

Das Programm News Agent dient der schnellen Zustellung der Nachrichten von Kaspersky Lab, der Benachrichtigung über das "Virus-Wetter" und über neu erschienene Nachrichten. Das Programm liest in vorgegebenen Zeitabständen von den Kaspersky-Lab-Newsservern eine Liste der verfügbaren Nachrichtenkanäle und der darin enthaltenen Informationen.

News Agent verfügt außerdem über folgende Funktionen:

- Visualisierung des Zustands des "Viren-Wetters" im Infobereich der Taskleiste von Microsoft Windows.
- Abonnieren und Abbestellen der Nachrichtenkanäle von Kaspersky Lab.
- Download von Nachrichten für jeden abonnierten Kanal in festgelegten Zeitabständen. Außerdem erfolgt eine Benachrichtigung über ungelesene Nachrichten.
- Anzeige von Nachrichten der abonnierten Kanäle.
- Anzeige einer Liste der Kanäle und ihrer Status.
- Öffnen der Webseite mit dem vollständigen Nachrichtentext im Browser.

News Agent funktioniert unter dem Betriebssystem Microsoft Windows. Er kann als separates Programm benutzt werden oder zu unterschiedlichen integrierten Lösungen von Kaspersky Lab gehören.

Kaspersky® OnLine Scanner

Dieses Programm ist ein kostenloser Dienst, der den Besuchern der Hersteller-Webseite zur Verfügung steht und die effektive Antiviren-Untersuchung des Computers im Online-Modus erlaubt. Kaspersky OnLine Scanner wird direkt im Browser ausgeführt. Dadurch kann der Benutzer schnell eine Antwort auf Fragen erhalten, die mit einer Infektion durch schädliche Programme verbunden sind. Im Rahmen der Untersuchung kann der Benutzer:

- Archive und Mail-Datenbanken von der Untersuchung ausschließen.
- standardmäßige oder erweiterte Datenbanken für die Untersuchung wählen.
- die Untersuchungsergebnisse in den Formaten txt und html in Berichten speichern.

Kaspersky® OnLine Scanner Pro

Dieses Programm stellt einen Abonnementsdienst dar, der den Besuchern der Hersteller-Webseite zur Verfügung steht und die effektive Antiviren-Untersuchung des Computers und die Desinfektion infizierter Dateien im Online-Modus erlaubt. Kaspersky OnLine Scanner Pro wird direkt im Browser ausgeführt. Im Rahmen der Untersuchung kann der Benutzer:

- Archive und Mail-Datenbanken von der Untersuchung ausschließen.
- standardmäßige oder erweiterte Datenbanken für die Untersuchung wählen.
- die Untersuchungsergebnisse in den Formaten txt und html in Berichten speichern.

Kaspersky® Internet Security 7.0

Kaspersky Internet Security 7.0 ist eine komplexe Lösung für den Schutz eines PCs vor den wichtigsten Bedrohungen (Viren, Hackerangriffe, Spam und Spyware), denen Informationen unterliegen. Alle Komponenten lassen sich über eine einheitliche Benutzeroberfläche einstellen und steuern.

Die Funktion des Antiviren-Schutzes umfasst:

- *Antiviren-Untersuchung des Mail-Datenstroms* auf Ebene des Datenübertragungsprotokolls (POP3, IMAP und NNTP für eingehende Mails und SMTP für ausgehende Mails) unabhängig vom verwendeten Mailprogramm. Für die populären Mailprogramme Microsoft Office Outlook, Microsoft Outlook Express und The Bat! sind Plug-ins und die Desinfektion von Mail-Datenbanken vorgesehen.

- *Antiviren-Untersuchung des Internet-Datenstroms*, der mit HTTP-Protokoll eintrifft, im Echtzeitschutz-Modus.
- *Schutz des Dateisystems*: Der Antiviren-Untersuchung können beliebige einzelne Dateien, Ordner und Laufwerke unterzogen werden. Außerdem sind vordefinierte Untersuchungsaufgaben für die Virenanalyse von kritischen Bereichen des Betriebssystems und von Objekten, die beim Start des Betriebssystem Microsoft Windows gestartet werden, vorhanden.
- *Proaktiver Schutz*: Das Programm führt die ununterbrochene Überwachung der Aktivität von Anwendungen und Prozessen durch, die im Arbeitsspeicher des Computers gestartet werden, verhindert gefährliche Veränderungen des Dateisystems und der Registrierung, und stellt das System nach schädlicher Einwirkung wieder her.

Der *Schutz vor Internetbetrug* beruht auf dem Erkennen von Phishing-Angriffen. Dadurch lässt sich der Diebstahl Ihrer vertraulichen Informationen verhindern (in erster Linie Kennwörter, Konto- und Kreditkartennummern, sowie Sperren der Ausführung gefährlicher Skripts auf Webseiten, Sperren von Popupfenstern und Werbebannern). Die Funktion zum *Sperren der automatischen Einwahl auf kostenpflichtige Internetressourcen* ermöglicht es, Programme zu identifizieren, die versuchen Ihr Modem für versteckte Verbindungen mit kostenpflichtigen Telefondiensten zu missbrauchen, indem diese Programme gesperrt werden. Das Modul *Schutz von vertraulichen Informationen* gewährleistet den Schutz vor dem unerlaubtem Zugriff und der Übertragung von Informationen mit vertraulichem Charakter. Die Komponente *Kindersicherung* bietet die Kontrolle über den Zugriff von Computerbenutzern auf Internetressourcen.

Kaspersky Internet Security 7.0 *erkennt Versuche zum Scannen der Ports Ihres Computers*, die häufig im Vorfeld von Netzwerkangriffen stattfinden, und wehrt bekannte Netzwerkangriffe erfolgreich ab. Auf der *Basis von vordefinierten Regeln* führt das Programm die Kontrolle aller Netzwerkaktionen durch und überwacht alle *eingehenden und ausgehenden Datenpakete*. Der Stealth-Modus *macht den Computer für die externe Umgebung praktisch unsichtbar*. In diesem Modus wird jede Netzwerkaktivität verboten, wenn sie nicht durch Ausnahmeregeln erlaubt wird, die vom Benutzer festgelegt wurden.

Im Programm wird eine komplexe Methode zur Spam-Filterung eingehender Mails angewandt:

- Untersuchung nach schwarzen und weißen Adressenlisten (einschließlich Adressen von Phishing-Seiten)
- Phrasenuntersuchung im Mailtext
- Analyse des Mailtexts mit Hilfe eines lernfähigen Algorithmus
- Erkennung von Spam in Form von Grafiken

Kaspersky Anti-Virus Mobile

Kaspersky Anti-Virus Mobile bietet den Antiviren-Schutz für mobile Geräte, die mit den Betriebssystemen Symbian OS und Microsoft Windows Mobile arbeiten. Das Programm erlaubt eine komplexe Antiviren-Untersuchung, die folgende Optionen umfasst:

- *Scan auf Befehl* des Arbeitsspeichers, der Speicherkarten, einzelner Ordner oder einer konkreten Datei eines mobilen Geräts. Beim Fund eines infizierten Objekts wird es in die Quarantäne verschoben oder gelöscht.
- *Echtzeit-Untersuchung*: Alle eingehenden und veränderten Objekte, sowie Dateien, auf die versucht wird zuzugreifen, werden automatisch untersucht.
- *Schutz vor sms- und mms-Spam*

Kaspersky Anti-Virus für Mail-Server

Das Produkt schützt die Dateisysteme von Servern, die unter den Betriebssystemen Microsoft Windows, Novell NetWare, Linux und Samba laufen, zuverlässig vor allen Arten schädlicher Programme. Das Produkt umfasst folgende Anwendungen von Kaspersky Lab:

- Kaspersky Administration Kit
- Kaspersky Anti-Virus for Windows Server
- Kaspersky Anti-Virus for Linux File Server
- Kaspersky Anti-Virus for Novell Netware
- Kaspersky Anti-Virus for Samba Server

Vorzüge und Funktionen:

- *Echtzeitschutz der Dateisysteme von Servern*: alle Dateien der Server werden untersucht, wenn versucht wird, sie zu öffnen und auf dem Server zu speichern.
- *Verhinderung von Viren-Epidemien*
- *Scan auf Befehl* des gesamten Dateisystems oder bestimmter Ordner und Dateien
- *Einsatz von Optimierungstechnologien* bei der Untersuchung von Objekten des Serverdateisystems
- *Systemwiederherstellung nach einer Infektion*
- *Skalierbarkeit* im Rahmen der verfügbaren Systemressourcen

- *Berücksichtigung der Systemauslastung*
- *Verwendung einer Liste mit vertrauenswürdigen Prozessen*, deren Aktivität auf dem Server nicht vom Programm kontrolliert wird.
- *Remote-Administration* des Produkts, einschließlich zentraler Installation, Konfiguration und Steuerung
- *Speicherung von Sicherungskopien infizierter und gelöschter Objekte*, um sie bei Bedarf wiederherzustellen.
- *Isolierung verdächtiger Objekte* in einem speziellen Speicher
- *Benachrichtigungen über Ereignisse* bei der Arbeit des Produkts für den Systemadministrator
- *Ausführliche Berichtsführung*
- *Automatisches Update der Datenbanken* des Softwareprodukts

Kaspersky Open Space Security

Kaspersky Open Space Security realisiert eine neue Art des Herangehens an die Sicherheit moderner Unternehmensnetzwerke mit beliebigem Umfang. Dabei gewährleistet es den zentralen Schutz von Informationssystemen und unterstützt externe Arbeitsplätze und mobile Benutzer.

Das Softwareprodukt umfasst vier Produkte:

- Kaspersky Work Space Security
- Kaspersky Business Space Security
- Kaspersky Enterprise Space Security
- Kaspersky Total Space Security

Im Folgenden wird jedes Produkt genau beschrieben.

Kaspersky Work Space Security bietet den zentralen Schutz von Workstations innerhalb und außerhalb eines Unternehmensnetzwerks. Es schützt vor allen aktuellen Internet-Bedrohungen wie Viren, Spyware, Hackerangriffen und Spam.

Vorzüge und Funktionen:

- *Komplexer Schutz vor Viren, Spyware, Hackerangriffen und Spam*
- *Proaktiver Schutz* vor neuen Schadprogrammen, die noch nicht in die Datenbanken aufgenommen wurden.
- *Personal Firewall* mit IDS/IPS-System
- *Rollback-Funktion für schädliche Veränderungen im System*

- *Schutz vor Phishing-Angriffen und Spam*
- *Dynamisches Ressourcen-Management* bei der vollständigen Untersuchung des Systems
- *Remote-Administration* des Produkts, einschließlich zentraler Installation, Konfiguration und Steuerung
- *Unterstützung von Cisco® NAC* (Network Admission Control)
- *Untersuchung von E-Mails und Internet-Traffic in Echtzeit*
- *Sperren von Popupfenstern und Werbebannern bei der Arbeit im Internet*
- *Sichere Arbeit in Netzwerken aller Art*, einschließlich Wi-Fi
- *Mittel zum Erstellen einer Notfall-CD zur Systemwiederherstellung*, um die Folgen von Virenangriffen zu beheben.
- *Flexibles Informationssystem* für den Schutzstatus
- *Automatisches Update der Datenbanken*
- *Vollständige Unterstützung von 64-Bit-Betriebssystemen*
- *Optimiert für Notebooks* mit Intel® Centrino® Duo
- *Möglichkeit zur Remote-Reparatur* (Intel® Active Management - Intel® vPro™)

Kaspersky Business Space Security bietet den optimalen Schutz für die Informationsressourcen einer Firma vor Internet-Bedrohungen. Es schützt Workstations und Dateiserver vor Viren, Trojanern und Würmern, und verhindert Virus-Epidemien. Zudem überwacht es die Integrität der Daten und ermöglicht den Benutzern den schnellen Zugriff auf Netzwerkressourcen.

Vorzüge und Funktionen:

- *Remote-Administration* des Produkts, einschließlich zentraler Installation, Konfiguration und Steuerung
- *Unterstützung von Cisco® NAC* (Network Admission Control);
- *Schutz von Workstations und Dateiservern vor allen Internet-Bedrohungen*
- *Verwendung der iSwift-Technologie zur Vermeidung wiederholter Untersuchungen* innerhalb eines Netzwerks
- *Dynamische Auslastung der Serverprozessoren*
- *Isolierung verdächtiger Objekte in einem speziellen Speicher*

- *Rollback-Funktion für schädliche Veränderungen im System*
- *Skalierbarkeit im Rahmen der verfügbaren Systemressourcen*
- *Proaktiver Schutz* für Workstations vor neuen Schadprogrammen, die noch nicht in die Datenbanken aufgenommen wurden.
- *Untersuchung von E-Mail und Internet-Traffic in Echtzeit*
- *Personal Firewall* mit IDS/IPS-System
- *Schutz bei der Arbeit in Wi-Fi-Netzwerken*
- *Technologie zum Selbstschutz des Antiviren-Programms vor Schadprogrammen*
- *Isolierung verdächtiger Objekte in einem speziellen Speicher*
- *Automatisches Update der Datenbanken*

Kaspersky Enterprise Space Security

Das Produkt umfasst Komponenten zum Schutz von Workstations und Groupware-Servern vor allen aktuellen Internet-Gefahren. Viren werden aus dem E-Mail-Datenstrom gelöscht. Die Integrität der Daten sowie die schnelle und sichere Verfügbarkeit der Netzwerkressourcen werden gewährleistet.

Vorzüge und Funktionen:

- *Schutz für Workstations und Server vor Viren, Trojanern und Würmern*
- *Schutz der Mailserver Sendmail, Qmail, Postfix und Exim*
- *Untersuchung aller E-Mails auf einem Microsoft Exchange Server*, einschließlich der gemeinsamen Ordner
- *Bearbeitung von E-Mails, Datenbanken und anderen Objekten auf Lotus Notes/Domino-Servern*
- *Schutz vor Phishing-Angriffen und Spam*
- *Verhinderung von massenhaften E-Mails und Viren-Epidemien*
- *Skalierbarkeit im Rahmen der verfügbaren Systemressourcen*
- *Remote-Administration* des Produkts, einschließlich zentraler Installation, Konfiguration und Steuerung
- *Unterstützung von Cisco® NAC* (Network Admission Control);
- *Proaktiver Schutz* für Workstations vor neuen Schadprogrammen, die noch nicht in die Datenbanken aufgenommen wurden.

- *Personal Firewall* mit IDS/IPS-System
- *Schutz bei der Arbeit in Wi-Fi-Netzwerken*
- *Untersuchung des Internet-Traffics in Echtzeit*
- *Rollback-Funktion für schädliche Veränderungen im System*
- *Dynamisches Ressourcen-Management* bei der vollständigen Untersuchung des Systems
- *Isolierung verdächtiger Objekte in einem speziellen Speicher*
- *Berichtssystem über den Status des Schutzsystems*
- *Automatisches Update der Datenbanken*

Kaspersky Total Space Security

Diese Lösung überwacht alle ein- und ausgehenden Datenströme, E-Mails, Internet-Traffic und alle Netzwerkaktionen. Kaspersky Total Space Security umfasst Komponenten zum Schutz von Workstations und mobilen Geräten, gewährleistet den schnellen und sicheren Zugriff der Anwender auf die Informationsressourcen der Firma und auf das Internet. Außerdem garantiert es Sicherheit bei der Kommunikation per E-Mail.

Vorzüge und Funktionen:

- *Komplexer Schutz vor Viren, Spyware, Hackerangriffen und Spam* auf allen Ebenen eines Unternehmensnetzwerks von der Workstation bis zur Internet-Gateway.
- *Proaktiver Schutz* für Workstations vor neuen Schadprogrammen, die noch nicht in die Datenbanken aufgenommen wurden.
- *Schutz für Mailserver und Groupware-Server*
- *Echtzeit-Untersuchung des Internet-Datenverkehrs* (HTTP/FTP), der in ein lokales Netzwerk eintrifft.
- *Skalierbarkeit im Rahmen der verfügbaren Systemressourcen*
- *Sperren des Zugriffs auf infizierte Workstations*
- *Verhinderung von Viren-Epidemien*
- *Zentrale Berichte über den Schutzstatus*
- *Remote-Administration* des Produkts, einschließlich zentraler Installation, Konfiguration und Steuerung
- *Unterstützung von Cisco® NAC* (Network Admission Control);
- *Unterstützung von Hardware-Proxyservern*

- *Filterung des Internet-Datenverkehrs* nach einer Liste vertrauenswürdiger Server, nach Objekttypen und nach Benutzergruppen
- *Verwendung der iSwift-Technologie zur Vermeidung wiederholter Untersuchungen* innerhalb eines Netzwerks
- *Dynamisches Ressourcen-Management* bei der vollständigen Untersuchung des Systems
- *Personal Firewall* mit IDS/IPS-System
- *Sichere Arbeit in Netzwerken aller Typen*, einschließlich Wi-Fi
- *Schutz vor Phishing-Angriffen und Spam*
- *Möglichkeit zur Remote-Reparatur* (Intel® Active Management - Intel® vPro™)
- *Rollback-Funktion für schädliche Veränderungen im System*
- *Technologie zum Selbstschutz des Antiviren-Programms vor Schadprogrammen*
- *Vollständige Unterstützung von 64-Bit-Betriebssystemen*
- *Automatisches Update der Datenbanken*

Kaspersky Security für Mail-Server

Kaspersky Security für Mail-Server schützt Mailserver und Groupware-Server gegen Schadprogramme und Spam. Das Produkt umfasst Anwendungen für den Schutz aller bekannten Mailserver wie Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix und Exim. Zudem kann auch ein separater Mail-Gateway organisiert werden. Zu dieser Lösung gehören:

- Kaspersky Administration Kit
- Kaspersky Mail Gateway
- Kaspersky Anti-Virus for Lotus Notes/Domino
- Kaspersky Anti-Virus for Microsoft Exchange
- Kaspersky Anti-Virus for Linux Mail Server

Funktionen:

- *Zuverlässiger Schutz vor schädlichen und potenziell gefährlichen Programmen*
- *Spam-Filterung*
- *Scan von ein- und ausgehenden E-Mails und E-Mail-Anhängen*

- *Antiviren-Untersuchung aller E-Mails auf einem Microsoft Exchange Server*, einschließlich der gemeinsamen Ordner
- *Untersuchung von E-Mails, Datenbanken und anderen Objekten auf Lotus Notes/Domino-Servern*
- *Filterung von E-Mails nach Typen der Anhänge*
- *Isolierung verdächtiger Objekte in einem speziellen Speicher*
- *Komfortable Bedienung*
- *Verhinderung von Viren-Epidemien*
- *Monitoring für den Status des Schutzsystems mit Hilfe von Benachrichtigungen*
- *Berichtsystem über die Arbeit der Anwendung*
- *Skalierbarkeit im Rahmen der verfügbaren Systemressourcen*
- *Automatisches Update der Datenbanken*

Kaspersky Security für Internet-Gateway

Das Produkt gewährleistet allen Mitarbeitern eines Unternehmens den sicheren Zugriff auf das Internet. Die Lösung löscht automatisch alle schädlichen und potenziell gefährlichen Programme aus dem Datenstrom, der über die Protokolle HTTP und FTP eintrifft. Das Produkt umfasst:

- Kaspersky Administration Kit
- Kaspersky Anti-Virus for Proxy Server
- Kaspersky Anti-Virus for Microsoft ISA Server
- Kaspersky Anti-Virus for Check Point FireWall-1

Funktionen:

- *Zuverlässiger Schutz vor schädlichen und potenziell gefährlichen Programmen*
- *Echtzeit-Untersuchung des Internet-Datenverkehrs* (HTTP/FTP)
- *Filterung des Internet-Datenverkehrs* nach einer Liste vertrauenswürdiger Server, nach Objekttypen und nach Benutzergruppen
- *Isolierung verdächtiger Objekte* in einem speziellen Speicher
- *Komfortable Bedienung*
- *Berichtsystem über die Arbeit der Anwendung*

- *Unterstützung von Hardware-Proxyservern*
- *Skalierbarkeit im Rahmen der verfügbaren Systemressourcen*
- *Automatisches Update der Datenbanken*

Kaspersky® Anti-Spam

Kaspersky Anti-Spam ist die erste in Russland entwickelte Software zum Spam-Schutz von kleinen und mittleren Unternehmen. Das Programm vereint moderne Verfahren der Sprachanalyse für Informationen in Textform, sämtliche modernen Verfahren zum Filtern von E-Mails (einschließlich RBL-Listen und formeller Prüfung von Nachrichten) sowie eine einmalige Auswahl an Dienstprogrammen, durch die der Nutzer in die Lage versetzt wird, bis zu 95 % der unerwünschten Nachrichten zu identifizieren und zu eliminieren.

Kaspersky® Anti-Spam ist ein Filterprogramm, das, am "Eingang" des firmeninternen Netzwerks installiert, sämtliche eingehenden E-Mails auf Spam überprüft. Das Programm ist kompatibel mit jedem beliebigen Mailing-System und kann sowohl auf bereits funktionierenden als auch auf separaten Mailservern installiert werden.

Die tägliche Aktualisierung der Filterdatenbank mit Mustertexten aus unserem Sprachlabor garantiert eine hohe Effizienz des Produkts. Die Datenbank-Updates erscheinen alle 20 Minuten.

Kaspersky Anti-Virus® for MIMESweeper

Kaspersky Anti-Virus® for MIMESweeper bietet die Hochgeschwindigkeits-Antiviren-Untersuchung des Datenverkehrs auf Servern, die Clearswift MIMEsweeper for SMTP / Clearswift MIMEsweeper for Exchange / Clearswift MIMEsweeper for Web verwenden.

Das Programm besitzt die Form eines Plug-ins (Erweiterungsmoduls) und führt im Echtzeit-Modus die Antiviren-Untersuchung und die Bearbeitung der ein- und ausgehenden E-Mail-Nachrichten durch.

B.2. Kontaktinformationen

Sollten Sie weitere Informationen wünschen, wenden Sie sich bitte an unsere Vertriebspartner oder direkt an Kaspersky Lab. Wir werden Sie gern umfassend per Telefon oder E-Mail beraten.

Weitere Information erhalten Sie bei:

Kaspersky Labs GmbH

Steinheilstraße 13

85053 Ingolstadt

Technischer Support	Tel.: +49 (0) 841 98 18 90 Fax: +49 (0) 841 98 18 918 E-Mail: support@kaspersky.de
Allgemeine Informationen	WWW: http://www.kaspersky.com/de/ http://www.viruslist.com/de/
Feedback zu unseren Benutzerhandbüchern	docfeedback@kaspersky.com (Diese Adresse ist für Rückmeldungen über das Handbuch und elektronische Hilfesystem gedacht.)

ANHANG C. ENDBENUTZER-LIZENZVERTRAG FÜR DIE ERWORBENE KASPERSKY LAB SOFTWARE

WICHTIG - bitte sorgfältig lesen: Lesen Sie die in diesem KASPERSKY LAB Endbenutzer-Lizenzvertrag ("EULA") beschriebenen Rechte und Einschränkungen sorgfältig durch. Sie werden gebeten, die Bestimmungen des EULAs zu prüfen und ihnen zuzustimmen oder diese abzulehnen.

Indem Sie das Sicherheitsetikett auf der CD/DVD-Box aufreißen oder wenn Sie die SOFTWARE installieren, erklären Sie sich mit den Bestimmungen des EULAs einverstanden. Falls Sie mit den Bestimmungen des EULAs NICHT einverstanden sind, geben Sie die erworbene Software bitte innerhalb von 14 Tagen an die Einkaufsstelle zurück. Nach Eingabe des Aktivierungscodes ist eine Rückgabe der Software ausgeschlossen.

Jede Bezugnahme auf "Software" schließt den Aktivierungscode oder die Schlüsseldatei ein, den Sie von Kaspersky Lab als Teil der Software erhalten.

Dieser EULA ist ein rechtsgültiger Vertrag zwischen Ihnen, dem Besitzer eines Exemplars der SOFTWARE (entweder als natürlicher oder als juristischer Person) und KASPERSKY LAB. KASPERSKY LAB wird sich das exklusive Urheberrecht auf die Computersoftware (auf die Software und die Antiviren-Datenbanken) vorbehalten. Indem Sie die SOFTWARE installieren, erklären Sie sich damit einverstanden, durch die Bestimmungen dieses EULAs gebunden zu sein. Falls Sie den Bestimmungen dieses EULAs nicht zustimmen, sind Sie nicht berechtigt, die SOFTWARE zu installieren und zu verwenden.

Die SOFTWARE ist sowohl durch Urheberrechtsgesetze und internationale Urheberrechtsverträge als auch durch andere Gesetze und Vereinbarungen über geistiges Eigentum geschützt.

1. LIZENZEINRÄUMUNG. Durch diesen EULA werden Ihnen folgende Rechte eingeräumt:

- Sie sind berechtigt, eine Kopie der SOFTWARE auf einem einzigen Computer zu installieren und zu verwenden. Eine Mehrplatzlizenz der SOFTWARE, dürfen Sie auf so vielen Computern installieren, wie Sie Lizenzen erworben haben.

- Sie sind berechtigt, die installierte SOFTWARE gemäß den Bestimmungen dieses Vertrags zu benutzen. Das Recht, Aktualisierungen

(Updates) der SOFTWARE zu beziehen, besteht nur, wenn sie es mit dem Verkäufer der SOFTWARE vereinbart haben und nur für die vereinbarte Dauer. Wenn Sie aufgrund Kaufvertrags oder in sonstiger Weise berechtigt sind, Aktualisierungen zu beziehen, so gelten die Bestimmungen dieses Vertrags entsprechend für die aktualisierte SOFTWARE. Sie können diesen Vertrag jederzeit kündigen, indem Sie alle Kopien der Software und der Dokumentation zerstören.

2. EINSCHRÄNKUNGEN

• Einschränkungen im Hinblick auf Zurückentwicklung (Reverse Engineering), Dekompilierung und Disassemblierung. Sie sind nicht berechtigt, die SOFTWARE zurückzuentwickeln (Reverse Engineering), zu dekompilieren oder zu disassemblieren, es sei denn und nur insoweit, wie das anwendbare Recht, ungeachtet dieser Einschränkung, dies ausdrücklich gestattet. Sie sind nicht berechtigt, diese Software in automatischen, halbautomatischen oder manuellen Tools zu verwenden, welche dazu dienen, Virensignaturen, Virenerkennungsroutinen, sowie beliebige andere Daten oder Codes zum Erkennen von schädlichem Code oder Daten zu erstellen.

• Vermietung. Sie sind nicht berechtigt, die SOFTWARE zu vermieten, zu verleasen oder zu verleihen.

• Supportleistungen. Nach Kauf und Aktivierung der SOFTWARE erhalten Sie sofort das Recht auf die Supportleistungen für die beim Kauf der SOFTWARE oder unabhängig davon vereinbarte Dauer. Supportleistungen verstehen sich wie folgt:

– stündliche Updates der Antiviren-Datenbank
– kostenloses Updates der Software
– technische Unterstützung sowohl per e-Mail als auch per Telefon mit KASPERSKY LAB

3. KÜNDIGUNG. Unbeschadet sonstiger Rechte ist KASPERSKY LAB berechtigt, diesen EULA fristlos zu kündigen, sofern Sie gegen die Bestimmungen dieses EULAs verstoßen. In einem solchen Fall sind Sie verpflichtet, sämtliche Kopien der SOFTWARE und alle ihre Komponenten zu vernichten.

4. URHEBERRECHT. Das Urheberrecht auf die Software, die gedruckten Begleitmaterialien und jede Kopie der Software liegt bei Kaspersky Lab, soweit es durch die Veräußerung nicht erschöpft ist.

5. GEWÄHRLEISTUNG. Kaufvertragliche Gewährleistungsansprüche bestehen nur gegenüber dem Unternehmen oder der Person, von der Sie die Software gekauft haben. Mit diesem Lizenzvertrag ist keine Erweiterung der kaufrechtlichen Gewährleistung verbunden. Nur für den Fall, dass Sie die Software unmittelbar von Kaspersky Lab gekauft haben sollten, gilt: KASPERSKY LAB gewährleistet, dass:

• die SOFTWARE den Spezifikationen im wesentlichen entspricht.

• im Falle einer physikalischen Lieferung der Originaldatenträger frei von Material- und Herstellungsfehlern ist.

• das Programm korrekt auf den Datenträger aufgezeichnet ist, die Dokumentation sämtliche Informationen enthält, die KASPERSKY LAB für die Benutzung der Software für erforderlich hält.

• die SOFTWARE binnen 90 Tagen ab der ersten Installation oder dem ersten Download, falls richtig behandelt, der in der beiliegenden Dokumentation bestimmten Funktionalität entspricht und laut derer voll funktionsfähig ist.

Gewährleistungspflichtige Mängel werden von KASPERSKY LAB oder dessen Lieferanten nach Entdeckung, auf jeden Fall aber vor Ablauf von der Gewährleistungsfrist, dem Ermessen von Kaspersky Lab nach, durch Ersatz, Reparatur, Umtausch oder Rückzahlung beseitigt, falls eine Mangelrüge rechtzeitig an Kaspersky Lab oder dessen Lieferanten gerichtet wurde. KASPERSKY LAB oder dessen Lieferanten übernehmen keine Gewährleistung für Mängel, die auf andere als für die Software vorgesehenen Einsatzbedingungen, unsachgemäße Behandlung oder dergleichen zurückzuführen sind.

ALLE ANDERE GEWÄHRLEISTUNGEN UND BEDINGUNGEN, SEIEN SIE AUSDRÜCKLICH ODER KONKLUDENT, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF, (FALLS ZUTREFFEND) JEDE KONKLUDENTE GEWÄHRLEISTUNG IM HINBLICK AUF HANDELSÜBLICHKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, FAHRLÄSSIGKEIT ODER MANGELNDE FACHMÄNNISCHE BEMÜHUNGEN WERDEN VON KASPERSKY LAB ODER DESSEN LIEFERANTEN ABGELEHNT. ES BESTEHT EBENFALLS KEINE GEWÄHRLEISTUNG ODER BEDINGUNG VON RECHTSANSPRÜCHEN IN BEZUG AUF RECHTSINHABERSCHAFT, UNGESTÖRTES NUTZUNGVERGNÜGEN ODER NICHTVERLETZUNG VON RECHTEN DRITTER. DAS GESAMTE RISIKO, DAS BEI DER BENUTZUNG ODER LEISTUNG DER SOFTWARE ENTSTEHT, LIEGT BEI IHNEN.

6. AUSSCHLUSS DER HAFTUNG FÜR ALLE SCHÄDEN. SOWEIT GESETZLICH ZUGELASSEN, SIND KASPERSKY LAB ODER DESSEN LIEFERANTEN IN KEINEM FALL HAFTBAR FÜR IRGENDWELCHE FOLGE-, ZUFÄLLIGEN, DIREKTEN, INDIREKTEN, SPEZIELLEN, STRAFRECHTLICHEN ODER ANDEREN SCHÄDEN WELCHER ART AUCH IMMER (EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF SCHÄDEN AN PERSONEN ODER SACHEN, SCHÄDEN AUS ENTGANGENEM GEWINN, GESCHÄFTSUNTERBRECHUNG, VERLUST VON GESCHÄFTLICHEN INFORMATIONEN, FÜR DEN VERLUST VON PRIVATSPHÄRE, DIE UNMÖGLICHKEIT, EINE PFLICHT ZU ERFÜLLEN (EINSCHLIESSLICH GEMÄSS TREU UND GUTEN GLAUBENS ODER VERNÜNFTIGER ANGEMESSENER SORGFALT) ZU ERFÜLLEN, FÜR FAHRLÄSSIGKEIT ODER ANDERE VERMÖGENSSCHÄDEN), DIE AUS DER VERWENDUNG

DER SOFTWARE ODER DER TATSACHE, DASS SIE NICHT VERWENDET WERDEN KANN, RESULTIEREN ODER DAMIT IN ZUSAMMENHANG STEHEN, SELBST WENN KASPERSKY LAB ODER DESSEN LIEFERANTEN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WORDEN IST. DIESER HAFTUNGSAUSSCHLUSS FÜR SCHÄDEN GILT AUCH DANN, WENN ABHILFEMASSNAHMEN IHREN WESENTLICHEN ZWECK VERFEHLEN.

7. ANWENDBARES RECHT. Dieser Vertrag unterliegt dem Recht der Bundesrepublik Deutschland. Die Geltung des UN-Kaufrechts ist ausgeschlossen.